THE PERSISTENT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE DILEMMA: CAN THE DEPARTMENT OF DEFENSE ACHIEVE INFORMATION SUPERIORITY?

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

TODD C. HOGAN, MAJOR, USAF
B.A., Psychology, University of South Florida, Tampa, FL, 1993

Fort Leavenworth, Kansas
2007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-06-2007	Master's Thesis	Aug 2006 - Jun 2007

4. TITLE AND SUBTITLE
The Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Hogan, Todd C., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
1 Reynolds Ave.
Ft. Leavenworth, KS 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Joint Force commanders, military services and governmental agencies recently stated an operational requirement for a persistent intelligence, surveillance, and reconnaissance (ISR) capability. The need for persistence implies a need to detect, identify, and characterize change in a target's status anywhere, anytime, in any weather, with increasingly higher levels of fidelity. Persistent ISR is the ability to do this with sufficient timeliness and precision to achieve the Joint Force Commander's (JFC) objectives. The Global War on Terror's (GWOT) multitude of threats demands an ISR capability with the persistence to find, fix, and track single individuals in a crowd; locate camouflaged, concealed, or mobile weapons of mass destruction (WMDs); and monitor any area on the globe sufficiently enough that meaningful changes can be detected and correctly interpreted in near-real-time. The persistent ISR capability would provide combatant commanders with assured and continued observational access to the multitude of elusive adversaries operating in their area of responsibility. However, is the realization of persistence currently achievable in the Department of Defense (DoD)? Insufficient intelligence collection platforms coupled with convoluted command and control responsibilities currently limit the Department's capability to achieve persistence in the near term.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified	UU	88	

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Todd C. Hogan

Thesis Title: The Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority?

Approved by:

_____, Thesis Committee Chair
Jack D. Kem, Ph.D.

_____, Member
Russell H. Thaden, M.M.A.S.

_____, Member
Lt Col Steven E. Ramer, M.A.

Accepted this 15th day of June 2007 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE PERSISTENT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE DILEMMA: CAN THE DEPARTMENT OF DEFENSE ACHIEVE INFORMATION SUPERIORITY?, by Major Todd C. Hogan, 88 pages.

Joint Force commanders, military services and governmental agencies recently stated an operational requirement for a persistent intelligence, surveillance, and reconnaissance (ISR) capability. The need for persistence implies a need to detect, identify, and characterize change in a target's status anywhere, anytime, in any weather, with increasingly higher levels of fidelity. Persistent ISR is the ability to do this with sufficient timeliness and precision to achieve the Joint Force Commander's (JFC) objectives. The Global War on Terror's (GWOT) multitude of threats demands an ISR capability with the persistence to find, fix, and track single individuals in a crowd; locate camouflaged, concealed, or mobile weapons of mass destruction (WMDs); and monitor any area on the globe sufficiently enough that meaningful changes can be detected and correctly interpreted in near-real-time.

The persistent ISR capability would provide combatant commanders with assured and continued observational access to the multitude of elusive adversaries operating in their area of responsibility. However, is the realization of persistence currently achievable in the Department of Defense (DoD)? Insufficient intelligence collection platforms coupled with convoluted command and control responsibilities currently limit the Department's capability to achieve persistence in the near term.

ACKNOWLEDGMENT

For Jessica and the girls . . . there love and support is invaluable.

TABLE OF CONTENTS

Page

MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE ii

ABSTRACT iii

ACKNOWLEDGMENT iv

ACRONYMS vii

ILLUSTRATIONS ix

CHAPTER 1. INTRODUCTION 1

CHAPTER 2. LITERATURE REVIEW 9

CHAPTER 3. RESEARCH METHODOLOGY 13

CHAPTER 4. ANALYSIS 18

The Criticism: *The 9/11 Commission Report* 20
The Criticism: Additional Findings 22
Intelligence Operations in Operation Iraqi Freedom 24
Too Much Information, Not Enough Intelligence 24
Communication Breakdown 25
Service Stovepipes 26
The Persistent Intelligence, Surveillance, and Reconnaissance Gap 28
The Need for Additional Sensors 30
Broken Lines of Communication 30
Too Much Information, Not Enough Analysts 34
Security Issues 36
More Efficient Ways to Collect Information 37
Improving the Collection Cycle 37
Additional Sensors 38
Current Collection Assets 38
Satellites 39
Airborne Assets 39
Unmanned Aerial Vehicles 40
Non-Traditional Intelligence, Surveillance, and Reconnaissance 42
Human Intelligence 43
Individual Soldiers 44
Future Collection Assets 45
Unmanned Aerial Vehicles 45
Aerostat 47

Potential of Near Space....49
High Altitude Airships....51
High Altitude Balloons....53
Better Methods of Passing Information....55
Put One Agency in Charge....56
Director of National Intelligence....57
United States Strategic Command....57
United States Joint Forces Command....58
Title 10....61
Findings....63

CHAPTER 5. CONCLUSIONS AND RECOMMENDATIONS....65

Conclusions....65
Recommendations....66

REFERENCE LIST....72

INITIAL DISTRIBUTION LIST....77

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT....78

ACRONYMS

BDA	Bomb Damage Assessment
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance
CENTCOM	Central Command
CIA	Central Intelligence Agency
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
GWOT	Global War on Terror
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
ISR	Intelligence, Surveillance, and Reconnaissance
JFC	Joint Force Commander
JIC	Joint Integrating Concept
LTA	Lighter Than Air
MASINT	Measurements and Signals Intelligence
NSA	National Security Agency
NTISR	Non-traditional Intelligence, Surveillance, and Reconnaissance
OIF	Operation Iraqi Freedom
SIGINT	Signals Intelligence
UAV	Unmanned Aerial Vehicle
UCP	Unified Command Plan
USDI	Undersecretary of Defense for Intelligence

US	United States
USAF	United States Air Force
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
WMD	Weapons of Mass Destruction

ILLUSTRATIONS

Page

Figure 1. United States Air Force RQ-4 Global Hawk 46

Figure 2. Aerostat 47

Figure 3. United States Air Force U-2, Dragon Lady 51

Figure 4. High Altitude Airship 52

Figure 5. Artist's Conception of the High-Altitude Airship High-Altitude Balloon 54

CHAPTER 1

INTRODUCTION

> Know the enemy and know yourself; in a hundred battles you will never be in peril. (1971, 129)
>
> Sun Tzu, Art of War

> The art of war is simple enough. Find out where your enemy is. Get at him as soon as you can. Strike him as hard as you can, and keep moving. (Brinton 1941, 239)
>
> Ulysses S. Grant

America's true intelligence collection capability is shrouded in mystique, as it should be. The superpower's intelligence force is the subject of much public speculation and attention. Indeed, action novel authors repeatedly portray a perfect, omniscient system while Hollywood continually speculates for the public in repeated screenplays. In Touchstone Picture's 1998 movie *Enemy of the State*, Director Tony Scott portrayed an all-seeing eye capability worthy of the Department of Defense's (DoD) true efforts. This capability, while unrealistic, if truly acquired, would grant war fighters an incredible advantage over today's illusive enemies. Imagine being able to not only see your enemy continually, but being in their mental decision making process. Imagine knowing where they were going (location), why they were going there (purpose), and what they were going to do (intent). Due to the related complexity and cost, such a capability, if realized, will initially be realized only by a world superpower.

Some would argue that during the last half a century the definition of a superpower was a country that possessed a nuclear arsenal. However, today it may be the ability to collect, process, and disseminate pertinent information rapidly on a global scale.

The ability to collect intelligence on a global scale is akin to the power of having an all seeing eye. Recent conflicts have demonstrated the need for this capability. The enemy of the Cold War is no longer, but the enemy of the Global War on Terror (GWOT) is determined and smart. That enemy learned from the past and perfected the capability of becoming lost in the crowd. Gone are the days of utilizing United States (US) reconnaissance satellites to locate the Medina Division in Iraq. Now the US must utilize their vast collection capability to locate two men in a vehicle burying an improvised explosive device in the middle of Iraq at nighttime. A more worrisome scenario includes a terrorist in possession of Weapons of Mass Destruction (WMD) that infiltrated the US. Much like George Washington's irregulars utilizing guerilla warfare to help defeat the traditional armies of Britain, this dilemma has challenged the world's superpower and questioned its ability to adapt to the new contemporary operating environment. The superpower that can adapt its vast armies and intelligence networks to successfully combat this guerilla threat will prove victorious.

The US currently utilizes the tools of its vast Intelligence, Surveillance, and Reconnaissance (ISR) capability to plan, collect, analyze, and disseminate information on an enemy to a fielded war fighter or decision maker. The intent is to provide the fielded war fighter with ISR that is actionable in form. In other words, the intelligence must be relevant to a problem set and must drive the commander to some form of decision. ISR utilizes a vast array of assets to collect all-source intelligence to include imagery intelligence (IMINT), signals intelligence (SIGINT), and measurements and signals intelligence (MASINT) for situational awareness against a targeted enemy. The complexity of the process has driven the US Intelligence Enterprise to be quite large.

Indeed, the DoD's current ISR Enterprise has grown considerably from the initial Corona satellite program in 1959, and comprises a multitude of assets administered by military and other governmental organizations.

Although considerable design and expense efforts created a vast array of collection assets, the GWOT has uncovered limitations in the current ISR Enterprise while fighting an insurgent threat. Currently, there is a very limited capability to maintain consistent surveillance over targets for any length of time. The GWOT enemy is elusive and able to escape the current ISR architecture when being hunted. Indeed, Osama bin Laden was under US surveillance in the past but escaped due to a lack of a persistent capability. War fighters identified the ability to maintain constant surveillance over an elusive enemy as a critical requirement in defeating the GWOT enemy. The Defense establishment refers to this potentially transformational capability as persistent ISR; and combatant commanders, the services, and government and law enforcement agencies want it sooner rather than later. In fact, combatant commanders identified this requirement as critical to their war fighting efforts through Integrated Priority List submissions to the Chairman of the Joint Staff (Department of Defense 2006b, 3). The Integrated Priority List communicates to the Joint Staff what capabilities the combatant commanders need to successfully complete their mission. Therefore, the requirement is currently valid but the capability is wanting.

The need for persistence implies a need to detect, identify, and characterize change in a target's status anywhere, anytime, in any weather with increasingly higher levels of fidelity. Also referred to as pervasive knowledge, persistent stare, and persistent surveillance; persistent ISR is the ability to execute these tasks with sufficient timeliness

and precision to achieve a Joint Force Commander's (JFC) stated objectives (Department of Defense 2006a, 7). This new buzzword describes the requirement for future ISR capabilities to transform the manner in which intelligence is provided to fielded warfighters. This "perfect knowledge" implies that once a targeted enemy is located, it will be unable to hide or move from under the intelligence umbrella highlighting it. This uninterrupted contact with a targeted enemy will increase understanding, which in turn will enable a faster decision cycle to occur at all levels of command and, if required, enable the application of precision force to achieve the desired effect (Pendall 2005a, 41). Persistent ISR seeks to capture activity as it occurs; however, it does not necessarily mean the activity is recognized or understood at the time of collection (Department of Defense 2006a, 8). This understanding can occur later. However, the capability implies that raw information will be available to all users instantaneously; not only to an analyst in Washington, DC, but to the war fighter in a squalid police headquarters in Ramadi. The capability has the potential to integrate the human interface and various collection technologies and processes across formerly stove piped domains (Pendall 2005a, 1). This is the essence of the persistent ISR capability.

The core requirement of persistent ISR is to use enterprise systems to detect, collect, characterize, and disseminate activity in the battlespace. Detected change and anomalies will prompt action from decision makers. According to Major David W. Pendall, US Army, persistent ISR has three core components:

1. Multimode and multidimensional continuous collection across all battlespace environments (Sensing),

2. Near-real-time data and knowledge distribution via enterprise systems with tailored, user-defined presentation formats (Delivery),

3. Horizontal integration of data and advanced, distributed analytics (Sensemaking and Understanding).

Persistent surveillance will create enterprise (intelligence) data and understanding to support military operations in an unprecedented manner (Pendall 2005a, 42).

The GWOT's multitude of threats demands an ISR capability with the persistence to find, fix, and track single individuals in a crowd; locate camouflaged, concealed, or mobile WMD; and monitor any area on the globe sufficiently enough that meaningful changes can be detected and correctly interpreted in near-real-time (Department of Defense 2006a, 3). The current institution must release Cold War paradigms and commit to a national defense system with the ability to reorder intelligence information flow and distribute actionable intelligence immediately to the end user. This paradigm shift can represent one of the largest leaps in intelligence capability and credibility for warfighters frustrated by community stovepipes. A persistent ISR capability would provide combatant commanders, government agencies, and coalition partners with assured and continued observational access to the multitude of elusive adversaries operating in their area of responsibility. Tying in all the parts, systems, planning, and communication architectures required for persistent ISR is complex and yet undefined. However, this promising and transformational capability would grant a commander or decision maker an asymmetric advantage over any adversary faced. Acquiring it is truly the next step in technology for DoD's collection capability and one highly sought after. Therefore, to

define the problem of acquiring persistent ISR, one must analyze its three main parts: the adversary, environment, and insufficiencies in current intelligence capabilities.

The modern day adversary faced by coalition forces introduced numerous problems for the traditional intelligence collection paradigm. These adversaries fail to engage coalition forces as traditional military units and are therefore more difficult to detect. By definition, modern day adversaries can include state and non-state actors, trans-national threats, terrorists, insurgents, and drug cartels and their associated networks. The threat faced by the Joint Force is wide ranging and consists of traditional, disruptive, irregular, and catastrophic challenges. This plethora of threats has an ability to adapt asymmetrically to a superior military capability and the environment can aid their cause.

Insurgents utilize the environment to veil operations and combat US superiority via an asymmetric approach. They employ advanced camouflage, concealment, and deception techniques to veil activity and deny the ability to track them. In addition, they utilize sub-terrain and urban environments to conduct operations. Finally, the enemy can easily blend into the local population requiring friendly forces to go to exhaustive lengths to sort the good from the bad. All of these factors have presented a new problem set to the US intelligence community and represent a significant advantage for the adversary. Locating insurgents or other adversarial forces in their environment represent the largest problem for US forces.

Finally, the problem exists with the current US intelligence collection architecture. The current intelligence process construct is the process of developing raw information into finished intelligence for policymakers to use in decision making and

action. There are five steps which constitute the intelligence process: planning and direction, collection, processing, analysis and production, and dissemination (Joint Chiefs of Staff 2004, Chapter III 2, 7). The DoD designed the current intelligence architecture to combat a large Soviet threat and adaptation to current combatant commander requirements has been slow. Existing architecture is often disjointed, non-compatible, and stove-piped. Alterations in the intelligence process are required to streamline the "sensor to shooter" flow and craft operational intelligence. All these factors seriously complicate US collection efforts and highlight the importance of adapting and acquiring new technologies.

Funding is another obvious detractor from reaching system potential. Arguably the most cited problem to advanced capability, funding is a likely scapegoat. However, this thesis will not address funding due to the desire to remain process oriented. Besides, due to the often cited need for a greater intelligence capability as critical to success in the GWOT, additional funding is already flowing from Congress. Indeed, funding is critical and can help provide the advance in intelligence collection capability and the monetary requirement to redesign and alter existing processing, analysis, and dissemination architectures to reach full potential.

Can the DoD achieve a persistent ISR capability in the near term? What capabilities must it acquire to achieve persistent ISR or how must it alter current processes to enable the ISR Enterprise to achieve this goal? This thesis will argue that the DoD cannot achieve a persistent ISR capability in the near future due to the lack of sufficient intelligence collection platforms and the disjointed nature of the intelligence community's command and control infrastructure as a whole. Given the negative

connotation associated with this conclusion, the thesis will outline suggested recommendations for the milestones required to achieve an initial capability.

In drawing these conclusions, a number of assumptions are made. First of all, this thesis assumes that Joint Forces will be required to conduct future operations in complex, anti-access, and denial and deception environments. Given the current operating environment, it is safe to assume the challenges of the future. Secondly, this thesis assumes future funding is available to fund highlighted requirements to achieve the capability. Fiscal year 2007 funding does provide significant budgetary improvements over fiscal year 2006 for improvements to the ISR Enterprise so leadership currently supports vast improvement. In addition, US space superiority or unfettered access to space is assumed. Potential adversaries will likely challenge this access in future conflicts, however, this field of warfare is likely years away and countermeasures are likely already in place. Finally, this thesis must assume that government leadership will continue to support a fielding of the persistent ISR requirement.

This thesis is organized in five chapters. Following this "Introductory" chapter, a chapter on the literary review will address current academic research in the field. The "Methodology" chapter will outline how the thesis will research the problem of obtaining a persistent ISR capability. The "Analysis" chapter represents the bulk of the thesis and research conducted to analyze the problem. Finally, the conclusion is self evident and will outline the thesis in its entirety. In the following "Methodology" chapter, the thesis will succinctly outline the manner in which the research will be conducted. The purpose will be to provide an outline in which one will understand the thesis' scope and the manner in which the conclusion is derived.

CHAPTER 2

LITERATURE REVIEW

Acquiring a persistent ISR capability would represent a major strategic, operational, and tactical advantage for the US. But a persistent ISR capability is a large step from the DoD's current collection capability. Some in the defense community probably fail to believe the capability will exist during their military service, if not their lifetime. Currently seen as a futuristic dream, the concept is now being analyzed and dissected with aggressiveness. The GWOT definitely helps with progress. Are we closer than we think? Possibly; however, it is one thing to propose a roadmap to reach the goal; it is another to implement it across departments, services, combatant commands, networks, and collection controlling agencies. This thesis will analyze whether or not the DoD can achieve this capability in the near future. And if it is not achievable, what are the pieces critical to success, and what is required to achieve this great capability?

Current views on achieving persistent ISR center upon the unmanned aerial vehicle (UAV). The UAV burst onto the scene in the last five years to significantly impact the world of ISR. The capability is arguably already persistent in a limited scope. The United States Air Force's (USAF) Predator and Global Hawk, the US Army's Hunter and Raven, along with smaller systems employed by the sister services currently satisfy a significant portion of collection requirements in theater and the planned acquisitions for the force will take on even more. Most conceptual frameworks for persistent ISR focus on the UAV and rightly so. However, a true persistent ISR capability will require a much more robust collection of assets linked together. Other schools of thought embrace a near

space micro-satellite capability and others discuss the aerodrome. Great ideas abound but the most logical and integrated capability in the near term is the most beneficial to the country.

A review of the available information on persistent ISR leads to the conclusion that there is no definitive concept plan on how to achieve persistent ISR in the DoD. Given the infancy of the concept, available information leads one to understand how a capability might assist in achieving persistent ISR. It may also demonstrate how a restructuring of the intelligence cycle could help achieve persistent ISR. However, there is no holistic plan to demonstrate what is required and how it must integrate into the current capability to achieve persistent ISR. Indeed, the idea is new and the concept open to methods of transformation. A well-researched comprehensive plan could have significant impact throughout the defense community.

When opening the door on the US intelligence collection business, one obviously must be cognizant of classification issues. The vast majority of information pertaining to this capability is classified and sometimes compartmented. The challenge is to know what is classified and what is not for inclusion in this unclassified thesis. Luckily, this capability is currently a concept and, therefore, can be discussed to some extent in that context. This thesis aims to reference enough unclassified information via the internet and professional publications to accurately portray the issues and draw conclusions.

Given the newness of the persistent ISR concept, there is quite limited information currently published on the topic. This is especially true in regard to books. However, there are articles and internet sources to choose from. One significant source to draw from is the monthly *C4ISR Journal, The Journal of Net-Centric Warfare* by

DefenseNews. In addition, although just coming onto the scene, official DoD publications will be referenced to gather research to include the Joint Staff's *Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction Joint Integrating Concept* and *Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction Joint Integrating Concept* draft. Also referenced is a recent School of Advanced Military Studies graduate thesis titled *The Promise of Persistent Surveillance and Its Implications for the Common Operating Picture*, by Major David W. Pendall, US Army. The RAND Corporation concluded research pertaining to the USAF's ISR Enterprise. One such article is *Global Implications for the U.S. Air Force*, by Edward R. Harshberger. Finally, combatant commander's Operational Plans (OPLANs) and Concept Plans (CONPLANs) have the potential of providing some context to planned future use and integration of persistent ISR.

There are a limited number of books in which to reference. In their entirety, they only make indirect reference to persistent ISR but by in large, they do cite the need for the concept and will provide additional background and potential solutions. Some of these include: *Military Transformation: Current Issues in Intelligence, Surveillance, and Reconnaissance*, by Judy G.Chizek, Jennifer Elsea, Richard A. Best, Jr., and Christopher Bolkcom; *Assuring Access in Key Strategic Regions, Toward a Long-Term Strategy* by Eric Larson and others; "Security and Defense in the Terrorist Era (Foreign Policy, Security, and Strategic Studies)," by Elinor C. Sloan; and *Operation Iraqi Freedom: What Went Right, What Went Wrong, and Why*, by Walter J. Boyne.

In summary, little is published on the persistent ISR concept. Therefore, the challenge will be conducting exhaustive research to gather as much information possible

to piece this thesis together. The majority of the information will likely exist in government and military related documents. Fortunately, expert sources on the topic seem willing to discuss the concept for the thesis in hopes that it will shed a sliver of light on courses of action for potential acquisition of the persistent ISR capability. Interviews with action officers from United States Strategic Command (USSTRATCOM), Central Command (CENTCOM), and the Joint Staff in addition to USAF experts will be included.

CHAPTER 3

RESEARCH METHODOLOGY

After conducting the literature review in chapter 2, chapter 3 will define the methods of research utilized in conducting this study and some key terms referred to in the thesis. The research question must be restated: Can the DoD achieve a persistent ISR capability in the near term? To adequately determine the factors critical to the DoD's desire to acquire persistence, this thesis will analyze the recent critiques of the US Intelligence Enterprise, specifically after 11 September and operations conducted during Operation Iraqi Freedom (OIF). This analysis will establish the issues the Enterprise must overcome in achieving persistence. After establishing the current capability, the thesis will establish a baseline from which to begin. The thesis will then analyze what must be accomplished to achieve a persistent ISR capability and conclude with recommendations.

This thesis will utilize a number of products, such as multiservice after action reviews, articles, theses, white papers, interviews, lessons learned reports, and commissioned studies to set the stage in exploring current US ISR capabilities. A determination of the 11 September findings and OIF ISR capability will define the starting point. Defining current capability will not be an easy determination, especially in the unclassified realm, but a general or adequate definition of a capability gap should be obtainable. This author will conduct an analysis of current information regarding persistent ISR to arrive at a conclusive determination of the required capability and the steps required to obtain it. This analysis will lead to the conclusions required to answer

the research question of whether or not the DoD can achieve a persistent ISR capability in the near future.

To ensure the reader fully comprehends the concepts presented in the body of the thesis, it is necessary to include some key definitions. To begin with, it is critical the reader understands the concept of ISR before arriving at an understanding of persistent ISR. Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations,* defines ISR as an activity that "synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operation. This is an integrated intelligence and operations function" (Joint Chiefs of Staff 2004, GL-18). ISR is a critical component of the larger intelligence process as a whole. The intelligence process (formerly known as the intelligence cycle) is "a process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback" (Joint Chiefs of Staff 2004, GL-18). There are many in government who utilize and rely on the intelligence process to do their jobs.

The intelligence community is a federation of executive branch agencies and organizations that conduct intelligence activities necessary for conduct of foreign relations and protection of national security. These organizations include the Central Intelligence Agency (CIA); Defense Intelligence Agency (DIA); National Reconnaissance Office; National Security Agency (NSA); National Geospatial-Intelligence Agency; State Department; Department of the Treasury; Department of

Homeland Security; Drug Enforcement Agency; Federal Bureau of Investigation; Department of Energy, and Service Intel Organizations (Army, Navy, USAF, Marines, and Coast Guard) (Department of Defense 2006a, 21).

A combination of some of these key terms defines the ISR Enterprise. The ISR Enterprise encompasses "those Defense organizations, resources, and personnel assigned responsibilities for executing any part of the intelligence mission. The ISR Enterprise includes a core set of organizations and resources that have intelligence as a primary function. The ISR Enterprise may include other resources providing information of intelligence value under command and control arrangements specified by the Combatant Commander, JFC, or subordinate/component commander" (Department of Defense 2006a, 21). Finally, intelligence preparation of the battlespace represents the manner in which military intelligence professionals analyze complex problems. Preparation of the battlespace is an analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database and analyzes it in detail to determine the impact of the enemy, environment, and terrain on operations, and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process (Joint Chiefs of Staff 2004, GL-18).

A keen understanding of the types of intelligence created by ISR is useful in drawing conclusions from this thesis**.** All-source intelligence encompasses "intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, IMINT, measurement and signature intelligence, signals intelligence, and open- source data in the production of

finished intelligence" (Joint Chiefs of Staff 2004, GL-10). The three key subsets identified above are human, imagery, and signals intelligence.

Human Intelligence (HUMINT) is "a category of intelligence derived from information collected and provided by human sources." IMINT is "intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media." SIGINT is "a category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted." One key subset of SIGINT is communications intelligence. Communications intelligence is "technical information and intelligence derived from foreign communications by other than the intended recipients" (Joint Chief of Staff 2004, GL 12-25). Finally, one key method of gaining intelligence on the battlefield is a relatively new concept and is currently in practice in OIF and Operation Enduring Freedom. Non-traditional ISR (NTISR) is the utilization of traditional warfighting systems as sensors in the collection of intelligence on the battlefield; for example, utilizing an F-16 targeting pod used to vector in laser guided bombs to collect enemy activity on the battlefield.

Finally, some of the key players affected by the Intelligence Enterprise need further clarification. The JFC is "a general term applied to a Combatant Commander, sub-unified commander, or joint task force commander authorized to exercise combatant command or operational control over a joint force" (Joint Chief of Staff 2001, 285). An insurgency is an "organized movement aimed at the overthrow of a constituted

government through use of subversion and armed conflict" (Joint Chief of Staff 2001, 265). Non-state actors, in international relations, are actors on the international level which are not states (Wikipedia, The Free Encyclopedia 2007a). State actors are persons who act on behalf of a governmental body (Wikipedia, The Free Encyclopedia 2007b). A transnational threat is any transnational activity (including international terrorism, narcotics trafficking, the proliferation of WMD, and the delivery systems for such weapons, and organized crime) that threatens the national security of the US (US Code, Title 50, 2006).

In the course of a thorough study of ISR capabilities and gaps during OIF, this thesis will form an understanding of near current ISR capabilities. A comparison of this capability versus the definition and assumed objectives for a persistent ISR capability will answer the research question posed of whether or not the DoD can achieve a persistent ISR capability. The next chapter will begin the thesis analysis and represents the bulk of the work. A summary of the thesis conclusions are contained in chapter 5.

CHAPTER 4

ANALYSIS

> The ability to continuously monitor a given target and provide immediate assessment of changes to it, known as Persistent ISR, is seen as essential to the transformed force's ability to defeat unconventional enemies like terrorists. (2001)
>
> General Richard B. Myers, USAF,
> Former Chairman, Joint Chiefs of Staff

> Have you noticed the tendency by the media to talk about intelligence failure? There is no intelligence failure in our country. There has been simply inadequate (use) of our intelligence bases. (2003)
>
> General Tommy Franks, USA, Retired

The following chapter will analyze the thesis research question of whether or not the DoD can achieve a persistent ISR capability in the near future. This thesis argues that the DoD cannot achieve a capability in the near future due to the lack of sufficient intelligence collection platforms and the disjointed nature of the intelligence community's command and control infrastructure as a whole. Chapter 4 will first discuss the criticism heaped upon the intelligence community after 11 September, and then discuss intelligence operations in support of OIF during 2003. The following section will analyze the persistent ISR "gap" and reveal some needed areas for improvement. Finally, the chapter will analyze how to achieve a persistent ISR capability by dissecting two suggested areas for improvement by the current USSTRATCOM Commander, General Cartwright. These areas focus on improving the ways DoD collects information and the manner in which it passes it. Both are critical to achieving the persistent capability.

It is no secret that significant improvements need to be made by the US intelligence community. While a much generalized statement that passes judgment on a large and complex enterprise, reforms are long overdue. Examples are easy to cite and the critiques are numerous. There are too many stovepipes, too many computer systems, architectures and programs, too many layers of classifications, and too many places to go to obtain the information one requires. It is no wonder it takes an individual at least ten to fifteen years to become proficient in the intelligence craft.

The current intelligence architecture is structured to combat a formidable Soviet Union threat in the less complicated world of the Cold War. Today's threat poses quite different challenges to the Intelligence Enterprise and requires revolutionary changes. The ability in which the ISR Enterprise can adapt to meet this threat will significantly impact the DoD's ability to achieve victory in the GWOT and America's future conflicts. According to security-studies expert Barry Posen, enhanced and effective intelligence operations are critical to countering terrorism and insurgency associated conflicts (Posen 2001/2002, 46). Indeed, the side capable of gaining the information edge will enjoy the upper hand. Therefore, making the needed refinements to the intelligence community is critical to success.

Identifying problems with an organization as large as the US intelligence community is both easy and difficult to do. It is similar to criticizing the health care system in the US; everyone has an opinion. However, this thesis will attempt to only restate well documented issues in identifying the core of the intelligence problem.

The Criticism: *The 9/11 Commission Report*

A well recognized and authoritative document illustrating the current issues with the intelligence organization is the *9/11 Commission Report* (National Commission on Terrorist Attacks 2004, 1). The report identified that a majority of the intelligence needed to uncover the 11 September plot was collected before the attack and resided in different US intelligence agencies at the time of attack. The critical links were simply not connected. The document identifies six problem areas in the intelligence community and recommends actions based on correcting them. The six problem areas were:

1. Structural barriers to performing joint intelligence work.
2. Lack of common standards and practices across the foreign-domestic divide.
3. Divided management of national intelligence capabilities.
4. Weak capacity to set priorities and move resources.
5. The Director of Central Intelligence has too many jobs.
6. Too complex and secret.

The first identified problem is arguably the most critical issue to deal with. This problem area states that the collection mission areas of the different agencies are aligned against their individual collection disciplines, or capabilities, and not the joint mission. Stated another way, the NSA focuses on SIGINT and the intelligence it can glean from that capability; not from what the joint combatant commanders need to accomplish their missions. This condition creates the legendary stovepipes of intelligence and often results in competition between the different intelligence organizations. For intelligence to truly be derived from all-source analysis, these stovepipes must be deconstructed and integrated.

Secondly, the Commission Report argues that intelligence products should include information fused from what is collected both overseas and domestically and intelligence professionals should be held to a common set of standards in their reporting. The third issue area speaks to the divide in intelligence organizations. Specifically, it describes how certain intelligence organizations have limited influence with other organizations due simply to their chain of command. An example is how the majority of intelligence agencies fall under the DoD but the CIA reports directly to the Director of National Intelligence. This limits the CIA's ability to influence, and sometimes coordinate with, DoD's agencies. The fourth issue argues that no one central national organization has the authority to reset national intelligence priorities and demand a reallocation of an agency's priorities for collection. The fifth argument is that the Director of Central Intelligence had too many jobs or wears too many hats. This issue was dealt with when the President instituted a Director of National Intelligence. Finally, the report opines that the US intelligence community has become so complex and convoluted that the different missions and the lanes in the road are fuzzy. Also, with intelligence budgets being largely classified, they are excused from scrutiny. There needs to be more oversight and efficiency (National Commission on Terrorist Attacks 2004, 408-10). The *9/11 Commission Report* provided great insight into the critical issues facing the community at the strategic level of intelligence. This focus area encapsulates the efforts and problems with the national intelligence community at the interagency level. One must also analyze intelligence at the operational level of warfare to discover deficiencies in providing support to the warfighter.

The Criticism: Additional Findings

While the *9/11 Commission Report* shed a significant amount of light on the issues in the intelligence community, many other commissions and reports analyzed additional issues. Another report addressing the processes involved in conducting global ISR looks at the core of the problem by succinctly identifying the genesis of the intelligence community and the challenges ahead.

> The individual organizations that comprise the National Intelligence Community (NIC), and their associated global ISR capabilities, were created primarily to work national strategic problem sets, not to support operational military commanders. Although these organizations have successfully provided critical support to military operations, they still function within the original strategic support construct. Most notably, their primary limitation is the inability to anticipate the operational commander's requirements based on a lack of understanding his commander's intent. Instead, these organizations tend to collect on particular targets and analyze the resulting intelligence based on the capabilities of the systems themselves. The result is voluminous amounts of data and information that must then be processed into intelligence. (Welch 2005, 3)

The above quote perhaps speaks more directly to the root of the problem: the design of the intelligence community and its inherent difficulty in supporting military operations. Indeed, the buzz term leading much of the intelligence community through the late nineties was "Intelligence Support to the Warfighter." This theme attempted, and somewhat succeeded, in refocusing the greater intelligence community on the need to support military decision makers in the field. From it, came another movement to declassify a majority of information, previously inaccessible to most military members, to make sure it was in the hands of someone who could utilize the information to affect change. This new mindset shook the community as it was forced to "loosen" control and change their ways. The community has come a long way through the last two decades, helped by a number of conflicts which tested and refined support concepts. While major

redesigns have not truly occurred since the Cold War structure was established, new processes were instituted to "patch" the holes and attempt to streamline processes. The alterations, however, are piecemeal and fail to realize the potential of change.

In 1996, the Defense Science Board investigated command, control communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) operations and submitted recommendations to the DoD. The Board recommended that national intelligence support be altered from a temporary, ad-hoc approach to a systematic method for supporting JFC requirements. The Board went on to recommend "DoD work with the National Intelligence Council to develop new ways of providing information support to operational commanders which effectively and efficiently integrates the rich array of assets available within the US and for DoD to develop mechanisms that facilitate the introduction of such revolutionary changes into warfighting capability" (Hermann and Welch 1997, 14-15). A revolutionary change is truly required in how intelligence organizations collect and distribute intelligence and provide support to military decision makers to focus collection where it is needed to achieve effects-based operations.

Indeed, the above mentioned conditions need to be overcome to help achieve a persistent ISR capability. OIF provides excellent insight into other problems with the Enterprise. Many of the issues experienced during OIF are directly attributed to the ones previously mentioned in the *9/11 Commission Report;* OIF merely highlighted them. During the rapid ground force drive north, Coalition forces outpaced their intelligence capability often times providing commanders with little, if any, intelligence information

on the threat they faced. The result was additional criticism heaped on the intelligence community throughout the DoD.

Intelligence Operations in Operation Iraqi Freedom

Coalition intelligence operations conducted during OIF illustrate the potential of tactically focused and integrated intelligence but more importantly, illustrate the great challenges still facing the community. The conflict likely witnessed the most spectacular intelligence collection operation ever conducted in the history of warfare. A total of eighty aircraft collected intelligence during the conflict. They included the RQ-1 Predator, EP-3, RC-135 Rivet Joint, P-3C Orion, U-2, E-8C Joint Surveillance Target and Radar System, and the RQ-4 Global Hawk which made its combat debut. These aircraft, plus some others, flew approximately 1,000 combat sorties and collected 3,200 hours of streaming video, 2,400 hours of SIGINT, and 42,000 battlefield images (Moseley 2003, 3). Success stories abound and new intelligence assets debuted new capabilities, but with the vast amount of collection assets available for utilization, weaknesses in the system also revealed themselves.

Too Much Information, Not Enough Intelligence

One weakness was the inability of analysts to sort through vast amounts of collected information, turn it into useful knowledge, and disseminate it to the warfighter in a timely manner. One example was the difficulty intelligence staffs had in providing accurate and timely bomb damage assessment to war planners (Bradley 2004, 6). This was complicated by the rapid movement of forces, however, the assessment process lagged behind the targeting cycle creating confusion and redundant effort. In addition,

ground units often did not have a concise read on where the enemy was along their axis of approach. This, too, was difficult due to the rapid ground advance and often resulted in ground maneuver units repeatedly conducting “movement to contact” operations, a type of operation they would rather not execute. The process during OIF was simply not able to maintain pace with ground maneuver units and their unquenched need for intelligence on the enemy (Bradley 2004, 8).

Information unfortunately cannot develop into “intelligence” without someone in the chain conducting “sense making” of the raw material. This process is known as the “production” portion of the intelligence cycle. Production occurs when analysts combine all the available information pertaining to an intelligence problem, analyze it, and make an assessment on a future course of action. Once the intelligence is disseminated, the commander in the field uses the assessment to plan his or her future course of action on the battlefield. To be effective, the analyst must know what the commander needs. If an analyst does not know the commander’s requirement, the potential for a critical vulnerability exists.

Communication Breakdown

Information is also often times collected without decision makers knowing of its existence. It could likely be valuable and or vital information to a commander in the field. An OIF example cites a target that was imaged by three different ISR assets from the previous day that could have satisfied a commander’s stated requirement, but it had not been analyzed and disseminated until it was of no further value (Bradley 2004, 8). This vignette explains a problem that likely occurs often in theater. There is voluminous amounts of collection, but it is either unavailable to all who require the intelligence or

they simply do not know where to acquire it. A flipside problem is when national agency analysts in the Washington, DC area capture information likely valuable to a combatant commander, they simply do not know who to send it too or the dissemination process the information is sent through takes so long that it is of no value when received.

When the USAF's RQ-4 Global Hawk's sortie capability increased in theater to fly almost daily sorties in either OIF or Operation Enduring Freedom, leadership at Beale AFB, California, put together a road show brief to educate fielded warfighters on the new capability. The platform made its debut during the initiation of hostilities and had been operating in theater for two years. However, upon receiving the brief detailing the platform's capabilities and access information, most Army leadership were stunned at its potential to affect operations. (Author's personal experience, March 2006, while stationed at the 9th Reconnaissance Wing, Beale AFB, California, which operates the RQ-4 and U-2 collection platforms.) The majority of collection managers knew the Global Hawk operated in theater but did not know how easily it could support them, how to request the support, or where to get its products. So much information is collected but, unfortunately, it is often undiscovered by those in need.

Service Stovepipes

Another OIF lesson learned was the inability of service-specific ISR assets and architectures to communicate with one another. The majority of intelligence collection systems and dissemination architectures were developed by the individual service with the communication integration between sister services occurring too late in the development game, if ever. This often results in an inability of the different services to coordinate collection operations and to be cognizant of one another's products. This also

fostered many of the so-called intelligence stovepipes lamented throughout the operational community. While there were success stories in OIF, this system development structural design unfortunately limits situational awareness and information sharing between the services. In addition, since the services conduct their own collection operations in a vacuum, it is a large reason why the Intelligence Enterprise is not as persistent as it could be.

One such incident involved the movement of five Iraqi Republican Guard Brigades and the failure of the intelligence community to identify their relocation before US forces engaged them. The units reportedly moved via nontraditional means utilizing civilian vehicles and leaving a large infrastructure behind to deceive Coalition Intelligence; it worked. To summarize the event, Major General John F. Kimmons, the J2 for CENTCOM during the war, provided these observations:

> You have to understand this unit was one of CENTCOM's targets, and its movement was completely missed by analysis. We owned the sky [Operation Southern and Northern Watch was ongoing] and had space support. We had repeated daily coverage on them. Yet, we never had the ability to recognize the change in density and match it to a baseline of data because the collection data resided in non-integrated databases. Thousands of heavy vehicles moved in broad daylight. We just couldn't see it with stove piped data sets; systemic human analyst searches missed it-we didn't have a near real time [machine data search and pattern recognition] capability. We should have had [automated] triggers in place to identify density change and trigger reporting thresholds. A computer could find it [density change] and we could leverage MASINT/EO/Spectral collection to compare and confirm. We did not have a baseline or history [digitally stored and easily retrievable] to compare to in this case. People just didn't think about it in this way. (Pendall 2000b, 13)

Major General Kimmons' quote highlights the inability of the Intelligence Enterprise to fuse information from different collection platforms due to their "non-integrated databases." The danger in not fixing this problem and achieving this capability is obvious. This is also a major hurdle in realizing a persistent ISR capability.

As stated earlier, the manner in which Coalition forces moved rapidly north toward Baghdad presented unanticipated challenges to the intelligence collection effort. Intelligence collection operations are focused on answering the commander's priority intelligence requirements, however, calls for tactical collection or time sensitive targets largely dislodged priority intelligence requirements satisfaction from the collection plan. Basically, the collection plan was reactive and responded to battlefield maneuver, not priorities the commander had set in place. This, in turn, made executing a synchronized and prioritized collection plan difficult for CENTCOM's collection managers.

While there was an unprecedented level of intelligence support and many success stories during OIF, an after-action review highlights the areas needed to improve upon to enable a persistent ISR capability. While US military commanders now have great fidelity of battlefield intelligence, the challenge is improving upon this capability and disseminating the information to fielded commanders that require it. Many required assets and architectures are in place, however, their inability to communicate in addition to command and control issues impede efficiency. The legacy of collecting intelligence during the Cold War is largely to blame. The community must now lay aside old paradigms to allow another revolution in military intelligence to occur.

The Persistent Intelligence, Surveillance, and Reconnaissance Gap

It is likely no surprise to the informed reader that the Intelligence Enterprise has room for improvement. Process alterations and new command structures are currently being implemented in order to address some of the issues previously referenced. When President Bush signed the *Unified Command Plan* (*UCP*) 2002, USSTRATCOM

received the new mission of responsible DoD agent for Global C4ISR (Myers, 2004). In addition, US Joint Forces Command's (USJFCOM) mission and focus morphed to concentrate on integrating joint warfighting techniques and capabilities, addressing policy and procedures, and championing technical system interoperability (US Congress, House 2004a, 1). The stated mission assignments present added potential for the ISR community. But are the new ideas, new command structures, new processes, and new leadership commonly focused on obtaining a persistent ISR capability? Again, a persistent ISR capability is being touted as the new dream ride of the enterprise and combatant commanders continue to call for this capability in their Integrated Priority Lists. There is a lot of discussion on persistent ISR and what it could help achieve in the GWOT but there seems to be limited initiatives aimed at actually achieving it. The time is ripe to improve the enterprise with the aim of achieving persistent ISR.

Why is the current US ISR capability not more persistent? What limits the Intelligence Enterprise from obtaining this capability now with the assets currently being operated? While necessary to identify the issues facing the intelligence community to set the groundwork, it is this gap in ISR capability that must be focused on to work towards obtaining a persistent ISR capability.

The current US ISR Enterprise has not realized its persistent potential due to a number of factors. The issues facing the intelligence community as a whole are, in essence, the issues impeding the realization of a persistent ISR capability. This problem set must be addressed in order to answer the challenge of the GWOT and its associated illusive enemy in addition to preparing the country for future conflict. There are four main barriers standing in the way of achieving persistence. These barriers include the

lack of sufficient collection sensors, broken intelligence lines of communication, too much information for available analysts to analyze, and security concerns.

The Need for Additional Sensors

To start, there are simply not enough surveillance and reconnaissance sensors in the DoD's inventory to be a persistent capability. This realization is evident with even an elementary study on intelligence collection. This is also clearly evident in the DoD's current limited ability to find and provide constant contact with an intelligence target. While the common integration of current systems and disciplines would greatly contribute to the capability, it is not enough. The utilization of UAVs is a relatively new technology and wartime employment tactics are still being developed. Employing fighter aircraft to conduct NTISR is also a comparatively new practice due to the recent integration of targeting pods capable of conducting ISR. New technologies are also under development to bring new capabilities to the warfighter and assist the ISR Enterprise. The further refinement and integration of these technologies has promise, however, they will not close the gap, and the key remains their synchronized integration into a net-centric information domain.

Broken Lines of Communication

The second issue is that communication lines from the collection assets to the end-user are not integrated and too numerous. General James E. Cartwright, US Marine Corps, the current Commander of USSTRATCOM, posited that only 25 to 30 percent of what is collected actually gets to the user (Martin 2007). This theory identifies an incredible need for process change and also cites the failure of waste in the intelligence

community. To a web savvy individual that works outside the intelligence community, it would make sense to have all available products in one centralized location for end user consumption. However, there are numerous locations on numerous systems with different classifications where an analyst can obtain information. The “process” is broken and too arduous.

Another area of needed improvement regarding communication lines is cross-cueing. The concept of cross-cueing implies an ability of one collection asset to “tip-off” or task another asset, usually from another discipline or with a different capability, in order to gain a more defined picture of the target. Currently, intelligence operators have limited success within a defined intelligence discipline area, like that of IMINT. As an example, operators can usually streamline the process of having a U-2 collect on a target that a Predator highlighted. The problem lies in reaching across disciplines. There is currently a distinct need for the ability to have a SIGINT platform collect on a target that an IMINT asset identified. There is simply a void in communication architecture linking the two different types of operators, especially when reaching across Services. This capability would greatly add fidelity to an intelligence target and contribute to a persistent ISR capability.

Another communication challenge to most in the intelligence community is the manner in which national intelligence collection is conducted. National collection refers to national intelligence agencies; such as NSA, CIA, and National Geospatial-Intelligence Agency, and the employment of their assets. The process for tasking and receiving national collection is highly structured and complicated. So much so that during times of crisis, these organizations must send representatives, in the form of a National

Intelligence Support Team, to the headquarters of the JFC to assist in the process. In addition, collection managers often utilize "owned" assets available to their JFC, even to the detriment of the final product, to satisfy collection requests solely based on the ease of the tasking process. If they own it, they can easily task it. National requests have a reputation as too time consuming and the process too cumbersome that by the time you received the requested product, it was often too late to be of use. This assumes approval for collection is even obtained. The tasking and successful collection by all available assets must be easier for over-tasked combatant command collection managers.

An additional communication breakdown involves the lack of communication amongst the individual services in the DoD. Each military service has an inherent intelligence collection capability to support their forces. The USAF has the majority of the collection capabilities, but each service has an impressive array of capabilities. The problem resides in the individual services' machine-to-machine interface capabilities. It is possible for an USAF Intelligence analyst to obtain US Army (USA) RC-7 SIGINT collected information, however, that individual would have to break down some doors to get the information, and if it is available, it would be quite difficult to locate. Therefore, if an USAF analyst is compiling information on a target and the USA's RC-7 collected valuable information on that target, it is quite likely the USAF analyst would never know of the Army's collection. Much cross-service success depends on established personal relationships. Chairman of the Joint Chiefs of Staff, General Richard Myers stated:

> I believe we depend in large measure on personal relationships and memoranda of understanding to force information-sharing across organizations and agencies. In fact, I've dropped a roll of duct tape on the podium during a speech to emphasize this point because, in a sense, we're duct taping together organizations and

> processes that weren't designed to be well-connected. We've made progress, but there's more to do. (US Congress, Senate 2004, 10)

Services purchase intelligence capabilities in order to enable their respected missions. While there are exceptions, the purpose of the majority of service related collection assets are to facilitate those services' forces in conducting their mission. Therefore, these assets and their associated communication infrastructures are tied into the service specific architectures. While there are starting to be more exceptions, rarely is thought conducted on how to tie a new capability into the joint community to facilitate joint intelligence operations. A persistent ISR capability would be more achievable if every DoD and National collection asset was at the JFC's disposal and their production was available across the intelligence domain. While the community is thinking more "joint" everyday, this integrated approach to acquisition and integration is currently unreachable.

A piece of the problem is likely attributed to the intelligence communities' current structure. The US employs sixteen total intelligence agencies; nine of which are in the DoD. These agencies are not forced to integrate their efforts, their products, or their communication architectures. This is due to the lack of a centralized authority ensuring the proper integration of effort to benefit the joint force. Therefore, if General Cartwright's statement is true, the end-user is able only to draw upon a quarter of the information available from the sixteen agencies to solve an intelligence problem. A better capability is achievable. This leads to the third reason why the current US intelligence community cannot currently achieve a persistent ISR capability.

Too Much Information, Not Enough Analysts

Another hurdle resides in the amount of information the community collects, the methods in which it is disseminated and correlated, and the manner in which it is turned into intelligence. The production of wine begins with the harvest. Usually, low paying laborers pick the grapes on the vine to initiate the transformation. But the critical work lies in the manner in which the grape juice is altered into fine wine. Anyone can make grape juice, but it takes an expert to make a fine California Cabernet. Especially if there are too many grapes for the number of wine makers on hand to produce wine.

The same concept applies to the intelligence business. It is both an art and a science, but it takes an expert to produce valuable and actionable intelligence. As previously stated, it can take years to train and season an intelligence analyst capable of providing valuable products. Also, flooding an analyst with too much information can make him or her quite ineffective. It is not the job of the intelligence analyst to "surf" intelligence webpages for information to fuse together into products. The same effect is produced by not providing the analyst all available information on a target so he or she can discern an all-source assessment of activity. These two issues speak to the intelligence community's need for additional analysts and better system integration to assist the analyst. Unfortunately, the analyst will likely continue to be challenged by both problem sets in the near future. Until the US can obtain a more effective intelligence collection and dissemination capability, the analyst will be faced with the challenge of not knowing if they have all available information (not knowing what one does not know) or not being able to sort through all available information in the time allotted (just

looking at what one has time for). A vicious cycle indeed; but must it be so complex? The crux of this problem is central to achieving a persistent ISR capability.

The majority of intelligence transformational discussions on persistent ISR center on the acquisition of new collection assets. Indeed, acquiring more persistent capabilities is critical to obtaining persistence over the battlefield to interpret terrorist plans and intentions. However, if there are not linear discussions focusing on funding the human and integration sides of the equation, the persistent ISR capability will fail to achieve the level of promise hoped for. The RAND Corporation published a report stating:

> Without concurrent investment in intelligence analysts and tools, moreover, the push for "persistent surveillance" in U.S. defense transformation discussions will not yield the level of insight into threat activities and behavior that current ISR systems suggest is possible. Increasing the efficiency of national security decision-making is not a product of linear increases in information or monitoring. (Tomes 2003, 21)

The "analysts and tools" pieces in the intelligence drive to obtain persistence are critical. Indeed, just producing more information via the revolutionary persistent capabilities outlined above does not produce intelligence. It produces more information. There is a difference. Henry Kissinger noted, "Since the mass of information available tends to exceed the capacity to evaluate it, a gap has opened up between information and knowledge and, even beyond that, between knowledge and wisdom" (2001, 284). If just more information is produced, does accomplishing this goal achieve the desired end state? Colonel Kevin Cunningham, former Dean of the US Army War College, concluded that, "the next generation of technical systems will be that much better at seeing, counting, and reporting; the success of doing so can breed misconceptions about the proper balance between technical and more manpower intensive intelligence support functions, including intelligence analysis. Having to contend with a higher volume of less

valuable information actually makes the analytic process less efficient" (Cunningham 2001, 19).

Transformational debates and discussions on persistent intelligence should focus on the requirement and acquisition of new and more persistent collection capabilities. However, if these discussions fail to acknowledge the need for additional analytical expertise coupled with critical system integration, they are off target (Cunningham 2001, 19). These attributes must be balanced in any persistent ISR approach.

Security Issues

Finally, a persistent ISR capability is difficult to acquire due to the multiple levels of security involved in collection assets and their products. Numerous levels of classification are dispersed on differently classified systems and only specific individuals have access to certain classifications. This inherently makes the process convoluted. The inherent problem is that this issue hampers who can talk to whom about what; therefore, it represents another break in communication. Communication is one of the key enabling capabilities of a persistent ISR capability.

The four outlined issues above represent a summary of the predicaments facing the ISR Enterprise and the challenges prohibiting a persistent ISR capability. General Cartwright, summed the issue up quite succinctly. He stated that the ISR community requires: (1) more efficient ways to collect information, (2) better ways to pass the information, and (3) better ways to store and manipulate the data (Martin 2007). General Cartwright is tasked with the responsibility of providing US ISR capabilities to combatant commanders worldwide so his assessment is an informed one and represents the efforts of his command to improve capabilities. In concentrating on the best manner

to obtain a persistent ISR capability, this thesis will analyze his first two requirements. These represent the keys to obtaining persistence; therefore, the focus will now switch to how to achieve a persistent ISR capability.

More Efficient Ways to Collect Information

General Cartwright's first requirement in improving ISR calls for more efficient ways to collect information. This requirement can be further broken up into two subordinate requirements. The first is better integration and efficiency in the current collection architecture. The second subordinate requirement is the need for additional collection capabilities. General Cartwright's second call for better ways to pass the information will be discussed later in the thesis.

Improving the Collection Cycle

Numerous references lead to the conclusion that more efficiency can be achieved in the current collection cycle through the integration and streamlining of current collection cycle practices. More system efficiency will lead to a more persistent capability. Recognizing the need for improvement, the Joint Staff recently attacked this exact problem and formulated the Persistent ISR Joint Integrating Concept (JIC) signed in February 2007. The JIC represents a Joint approach to integrating the planning and direction of ISR assets to achieve operational objectives for the JFC.

While the JIC "proposes to improve persistence through integrated, synchronized management in the planning and direction of ISR assets" for the 2014 to 2026 timeframe, it does not call for additional sensors (Department of Defense 2006b, 1). In addition, it does not propose enhancements to the processing, exploitation, analysis, and distribution

of sensor data, information, and finished intelligence. Therefore, it solely focuses on the planning and direction portion of the intelligence collection cycle.

The JIC recognizes faults in the current trend to acquire additional collection assets with little regard to how they integrate into the ISR Enterprise and calls for a paradigm shift. Integrating collection management functions and leveraging the current capabilities of the intelligence community is critical to realizing a fielded persistent capability (Department of Defense 2006b, 1). This historic effort will revolutionize the intelligence collection community across the services and enable significant strides in improving efficiency and synchronization. The significant scope of the effort is foreshadowed in the timeframe the JIC targets (2014 to 2026). Proposing such changes seven years in the future signifies the work to be done to realize the improved capability.

Additional Sensors

The second subordinate requirement is the need for additional collection capabilities. If the Intelligence Enterprise requires additional collection sensors, what kinds are essential to establishing a persistent capability? Promising technology is under development to complement and grow the current architecture. An analysis of current and potential collection capabilities will define the requirement.

Current Collection Assets

Current US collection assets employed by the US can be categorized into the following categories: satellites, aircraft, UAVs, NTISR assets, ground-based sensors, and individual Soldiers. Examples of potential sensors of the future include near-space balloons, microsats, and further refinement of the UAV. Each asset currently provides, or

promises, a unique capability to the enterprise. In addition, they also bring unique operating costs and integration architectures which further complicate the process; however, all are critical to the integrated requirement of decision superiority. The analysis of each capability will uncover future requirements of the Intelligence Enterprise.

Satellites

Reconnaissance satellites have long been the key strategic collection asset of the US. Operating since 1959, US reconnaissance satellites perform a number of functions to include the collection of IMINT, SIGINT, MASINT, strategy compliance, and others. The operational advantages to utilizing satellites include the lack of human risk, high resolution, relatively ease of maintenance, and speed of dissemination. However, the main limiting factor resides in the fact that a satellites' loiter time is limited due to orbital mechanics. Although in contrast to Hollywood's portrayed idyllic capability, satellites have an extremely limited time to focus on a target. This limiting factor is not correctable; it is simply physics. While critical to the Intelligence Enterprise, the satellite can only contribute to a portion of a future persistent ISR capability.

Airborne Assets

Airborne collection assets have a long and distinguished record of providing strategic, operational, and tactical intelligence to US decision makers dating back to 1956. Starting with the U-2 Dragon Lady, which is still in use today, US reconnaissance aircraft have a unique ability to be responsive to combatant commander's priority intelligence requirements. Although vulnerable to an enemy's air defenses, airborne

collection assets have proved elusive while operating high over enemy airspace or along international boundaries. All the while, they collect operational SIGINT and IMINT intelligence critical to US national objectives. Indeed, the U-2's discovery of Soviet missiles in Cuba in 1962, initiated thirteen days of history long to be forgotten.

These unique collection assets have proven incredibly valuable to piecing together critical intelligence information for more than fifty years. However, they are limited by the human component. The pilot can only remain airborne for a limited time, which in turn, limits their persistence. The asset can contribute to a persistent system; however, its limits coupled with an extreme operating cost and uncertain future, make this only a piece of the solution.

Unmanned Aerial Vehicles

The UAV is the airborne reconnaissance platform of the future. Also known as the Remotely Piloted Vehicle, or Drone, the UAV has only recently come into its own. Historically, utilizing unmanned platforms for reconnaissance purposes dates back to the 1960's with the production of the Ryan Firebee. This platform and its predecessors provided intelligence to military users throughout the Vietnam War and their wartime utility continues to grow today (Wikipedia, The Free Encyclopedia 2007c). Indeed, the future of the UAV portends to be limitless. Recent wartime utilization of the USAF Predator and Global Hawk along with the Army's Scout and Hunter vehicles proved incredible potential. One distinct advantage of employing the UAV is the risk factor. Removing the human factor from the cockpit provides added options for risk assumption not previously available. Risk aversion coupled with the larger UAV's endurance abilities highlight the platform's potential. With great endurance capabilities, the UAV provides

an aerial collection asset perfect for persistence. The USAF's Global Hawk system represents the cutting edge of unmanned reconnaissance technology. The system can remain airborne for 35 hours; reach a range of 12,000 nautical miles at altitudes up to 65,000 ft (United States Air Force 2007a). The Global Hawk system will garner almost one-half of the total US UAV sensor funding for at least the next few years in its quest to replace the aged U-2. It is also the only UAV program that will receive the same type of sensors identical to manned collection platforms (Rockwell 2005, 49). This capability, while still young, represents the foremost US collection asset in the race towards achieving persistence.

The DoD is purchasing UAVs in record numbers. Every service is acquiring systems to suit their individual needs. The USAF is purchasing systems for strategic, operational, and tactical support to combatant commanders, the Navy for fleet defense, and the Army and Marine Corps in support of ground forces. The USAF's U-2 Dragon Lady will be phased out and replaced by RQ-4 Global Hawks; the timing is still under debate (Dorr 2006). The Army is utilizing funding slated for a cancelled program to buy the Warrior Extended Range/Multi Purpose UAV, an armed Predator variant (Defense Industry Daily 2007). The next Predator, MQ-9 Reaper UAV, is currently being fielded and will be utilized as an armed hunter-killer vehicle (United States Air Force 2007b). Based on DoD's spending, UAVs are the wave of the future. With the projected numbers of sensors planned for fielding, the UAV will present a large collection portion of a future persistent ISR capability.

Non-Traditional Intelligence, Surveillance, and Reconnaissance

Another capability that shows promise is the utilization and integration of NTISR collectors. This capability is relatively new and came about from new technology integration that presented itself after fighter aircraft were upgraded with new and improved targeting pods capable of great resolution. These targeting pods enjoy a capability to witness activity on the ground and report it to decision makers, hence the non-traditional title. These systems can provide troops on the ground with instant situational awareness of an enemy, either directly or via the pilot. In fact, the top three new-generation targeting pods are now being marketed to military consumers as "targeting/ISR systems." In addition, the "Litening" targeting pod system now on many fighter aircraft and even the B-52 bomber has the ability via radio to transmit real-time video directly to troops on the ground. The ground receiver is the Remote Operations Video Enhanced Receiver, or ROVER, and its vast utility is greatly enhancing the Soldier's situational awareness when an aircraft loiters overhead (Rockwell 2005, 46).

Another benefit is NTISR's ability to provide battle damage assessment via video on demand. Post-strike, a pilot can image the struck target to provide accurate imagery to intelligence analysts for a post-strike assessment. This new technique of utilizing existing technologies for intelligence gathering saves money and vastly increases the eyes in the sky available for a JFC's assessment requirements (Tirpak 2006). The current fielding of the F/A-22 RAPTOR, the USAF's newest fighter aircraft, also presents new opportunities in providing NTISR to fielded commanders. The platform employs a powerful active electronically-scanned array radar for multipurpose combat but that also provides great sensor fidelity. The active electronically-scanned array radar can provide simultaneous

air-to-air tracking capabilities in addition to an air-to-ground imaging and ground moving target indicator tracking modes. This unique potential places a critical collection asset onboard a stealthy aircraft capable of collecting where no other airborne asset could previously penetrate (Committee on C4ISR 2006, 198). The potential ISR abilities of the active electronically-scanned array radar will also be fielded on future aircraft like the Joint Strike Fighter which greatly increases sensors over a battlefield. The obvious detractor from this capability, similar to others, is the limited loiter time available from the asset. However, if properly integrated, NTISR can be a force enabler to the JFC's intelligence staff and a persistent capability.

Human Intelligence

The drive for persistence as a concept places great emphasis on a technological advantage, however, it does not solely rely on advanced sensors. HUMINT, is the oldest form of intelligence gathering and can provide the simplest form of a long-term dwell capability on a target. As Vice Admiral Jacoby (Director, Defense Intelligence Agency from July 2002 to November 2005) stated, "A HUMINT asset may prove to be the best way to dwell on a particular problem. It is about an integrated collection approach, with the end result being persistence in your ability to stay with the problem as long as it takes to understand it" (Pendall 2005b, 26). HUMINT capabilities were recognized as needing attention after 11 September, and the DoD is emphasizing and funding new capabilities in this realm.

Individual Soldiers

The last collection asset currently fielded is the individual Soldier. Soldiers have been utilized as intelligence gatherers for centuries. Recently though, a campaign has swept the DoD emphasizing the ability of every Soldier to collect enemy information. This campaign can be attributed to the GWOT's asymmetrical threat and the requirement for increased awareness. A campaign like the Army's "Every Soldier is a Sensor (ES2)" and the USAF's "Eagle Eyes" program, trains Soldiers to be suspicious and report unusual activity gleaned from street patrols or tactical operations. This type of sensor utilization is especially advantageous when coupled with additional information to piece intelligence together. If emphasized and instructed, the program can greatly increase a JFC's available sensor pool.

The current US intelligence collection enterprise is robust and has provided the means to affect military and diplomatic operations shaping the modern day world. But is this capability sufficient to transition the enterprise to that of persistence? The answer is obviously no due to combatant commander's continuing call for a persistent capability. New and more efficient collection technologies are warranted for persistence. Indeed, US military services must always seek, research, develop, and field the latest in military technology to ensure a technological edge is maintained over the world's adversaries. Therefore, US collection assets must utilize new frontiers and technologies to provide decision-makers with the most robust and accurate information possible to affect operations. These new capabilities represent the future of ISR collection operations and, if properly developed, will have the potential to provide the US with a persistent capability

Future Collection Assets

The ISR platforms of the future will utilize advancements in technology at a rate unseen in the history of warfare. To most, the capabilities of the armed Predator still boggle the mind. But tomorrow's capabilities promise amazing capability, efficiency, and lower cost. The challenge will lie in the DoD's ability to adapt rapidly enough to remain in stride with available technology. Future fielded collection technologies will likely be smaller, more elusive to an adversary all while providing greater fidelity of collection. The continued refinement of the UAV will be the most immediately utilized collection asset of the future.

Unmanned Aerial Vehicles

The UAV is still a relatively new collection asset in modern day warfare. Today's larger UAVs, like the USAF's Global Hawk (see figure 1) or Predator, are considered low-density, high-demand assets due to their low numbers and high cost. A single Global Hawk UAV costs almost $60 million making the vehicle five times its originally projected cost. That price is twice as expensive as an F-16. The ability to employ these assets in a high threat tactical environment will be limited in the future due to able air defense systems or directed energy weapons. Even with its full allotment of projected airframes, the USAF could simply not afford to employ these assets in attritional warfare against a country with modern day air defense equipment. The cost would be too high for a combatant commander (Abatti 2005, 10).

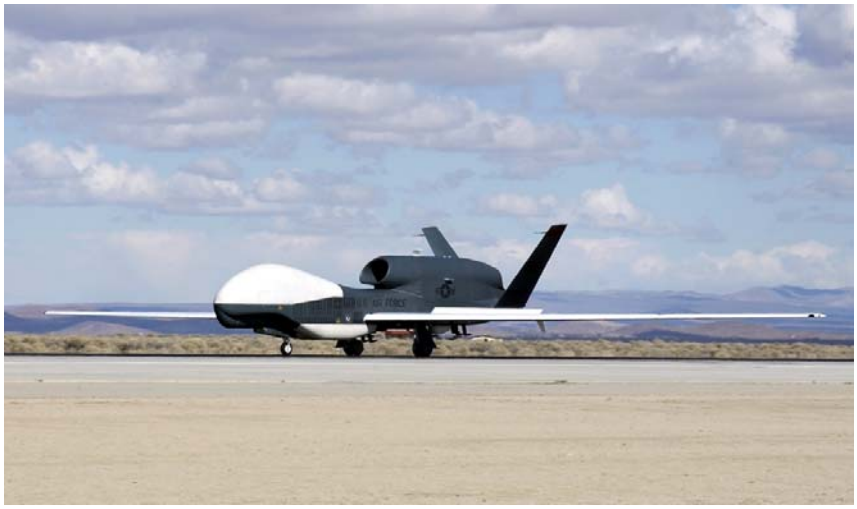


Figure 1. United States Air Force RQ-4 Global Hawk
Source: United States Air Force, Photo by Chad Bellay; available from http://www.af.mil/photos/index.asp?galleryID=47&page=1; Internet; accessed on 25 May 2007.

Future developmental efforts will provide a less expensive, smaller UAV capable of "swarming" over targets to provide a persistent capability. These micro UAVs will likely see expanded mission sets to include WMD location, Suppression of Enemy Air Defense operations, electronic warfare, bomb damage assessment (BDA), and strike missions. Their potential to affect full spectrum operations will change the manner in which warfare is waged (Abatti 2005, 27).

One emerging role for tomorrow's UAVs is BDA. The USAF Research Laboratory Munitions Directorate plans to demonstrate the use of a micro UAV for "instant BDA." The micro UAV would be released at a pre-selected altitude from a guided bomb. As the bomb impacts the target, the micro UAV would orbit and transmit post-strike images to a command facility to determine strike affects. If the mission failed to achieve the desired result, the aircraft could simply restrike the target on the same sortie. Researchers also theorize that the same micro-UAV could then land and crawl into

the target remains to determine true strike affects. Better yet, they could also take air samples to extract any chemical release into the air to determine WMD contaminates. While futuristic in nature, the capabilities of these micro UAVs will be beyond comprehension by 2025 (Abatti 2005, 29). According to Dr. Bushnell, NASA's Chief Scientist, by 2025 the world will be full of "Wondrous/Ubiquitous land/sea/air/space multiphysics/hyperspectral sensor swarms" (Abatti 2005, 34).

Aerostat

Aerostats have been utilized throughout history for military surveillance and anti-submarine warfare. This type of asset is classified as a "lighter than air (LTA)" aircraft capable of remaining aloft for prolonged periods. Aerostats are usually tethered to the ground and remain stationary in space. Envision the "Goodyear Blimp" with military utility (see figure 2).

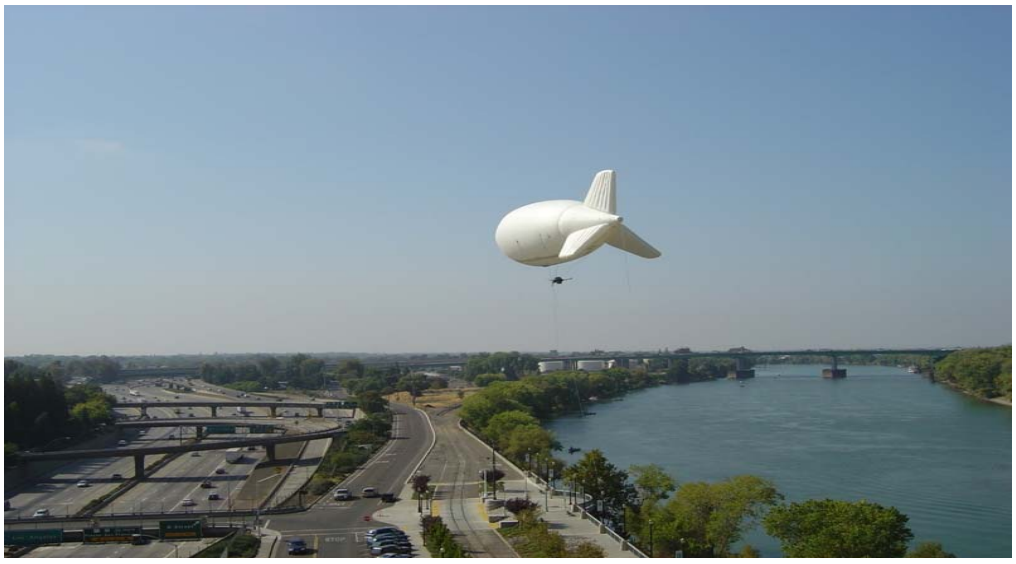


Figure 2. Aerostat
Source: TopIVision.com, Images; available from http://www.topivision.com/Images/Aerostat/2.jpg; Internet; accessed on 25 May 2007.

The US Navy disbanded their last airship unit in 1962, but the USAF still operates a dozen aerostats today. These are mainly operated along the US border to monitor drug trafficking. The Army recently deployed two different types of aerostats equipped with ground surveillance equipment to Afghanistan for force protection purposes with significant success (Bolkcom 2004, 1-2). In addition, the Marine Corps showcased the MRAID, or Marine Rapid Aerostat Initial Deployment, in pre-deployment training in Spring, 2006. MRAID deploys infrared, video, and communication sensors to an altitude of 5,000 feet to provide intelligence, surveillance, and force protection in urban environments (Rowe 2006, 32). Recent technological developments, coupled with a decreased air threat to US airborne assets, have shed light on potential LTA utility in pursuit of a more persistent ISR capability.

Aerostats appear perfectly suited for providing a persistent ISR capability over a limited portion of the battlefield. The most developed LTA program is the USAF's Tethered Aerostat Radar System that has operated since 1980 along the US border and Caribbean in a drug interdiction role. The Tethered Aerostat Radar System can lift 2,200 pounds of sensor to 12,000 feet and detect targets out to 200 miles, all while remaining aloft for months on end (United States Air Force 2007d). Defense Advanced Research Projects Agency is also currently working on a stratospheric airship sensor that can remain airborne for years (Bolkcom 2004, 1-2). Until this stratospheric aerostat is realized, the current Tethered Aerostat Radar System platform altitude ceiling parameters limit aerostats to providing limited coverage of a theater. Another disadvantage is potential vulnerability to enemy ground fire. However, the aerostat is the most developed and mature LTA system and can provide a persistent capability at a low cost with long

dwell times. If the DoD grasps this capability and develops it further, the potential for aerostats to provide a persistent ISR capability is great; especially in the force protection role.

Potential of Near Space

One of the most exciting environments virtually unexplored by man is the potential for operations in an area known as near-space. Near-space is the environment that spans from an altitude of about 12 miles (close to the internationally accepted upper limit of controlled airspace) and 62 miles (loosely defined as the lower limit of space). Until now, this area has virtually been untouched, yet it represents an incredibly rich environment from which to exploit potential persistent ISR in addition to other sought after capabilities. This "no man's land" is such due to two limiting factors. The air is too thin to support aircraft yet gravity is too strong to sustain a satellite's required orbit (Stephens 2005). Yet, the USAF is pursuing capabilities that could populate this area with balloons, high-altitude airships, and aerostats. In fact, the USAF deems it so important; its Near-Space Access Program is operated by its own High-Altitude Balloon and Tethered Aerostat Group in the Air Force Research Laboratory Space Vehicles Directorate, Kirtland AFB, New Mexico (Stephens 2005).

There are many reasons for this research full-court press. The first is due to the expense factor; building and launching these assets into near-space is considerably less expensive than most ISR capabilities currently employed. The infrastructure required is considerably less technologically demanding and therefore, less expensive. In addition, launching assets into near-space is incredibly responsive when compared to the time it takes to launch a satellite and or reconnaissance aircraft. In terms of safety, there is

currently no known threat to assets that could potentially operate in near-space; therefore, the risk is low. Current research is largely utilizing off-the-shelf technologies to draw from ongoing commercial sector experimentation. This not only saves already stretched budgets, but time. For the potential to collect ISR requirements, the vehicles would be approximately twenty times closer to earth than low-earth orbit satellites; a significant enhancement which would offer larger coverage areas for sensors (Stephens 2005). Finally, and more importantly, the potential loiter time available to assets operating in near-space is virtually limitless when compared to current capabilities. The U-2 (see figure 3) with many expensive upgrades integrated over the years, fills the niche of a responsive, high altitude reconnaissance asset for the military. However, missions cannot extend much longer than 10 hours flight time and even less collection time. Near-space vehicles could “stare” at an area unblinkingly for months at a time. While there are barriers to near-space employment, the potential is great and with the impact of ongoing research, asset employment should be achievable in the near term.

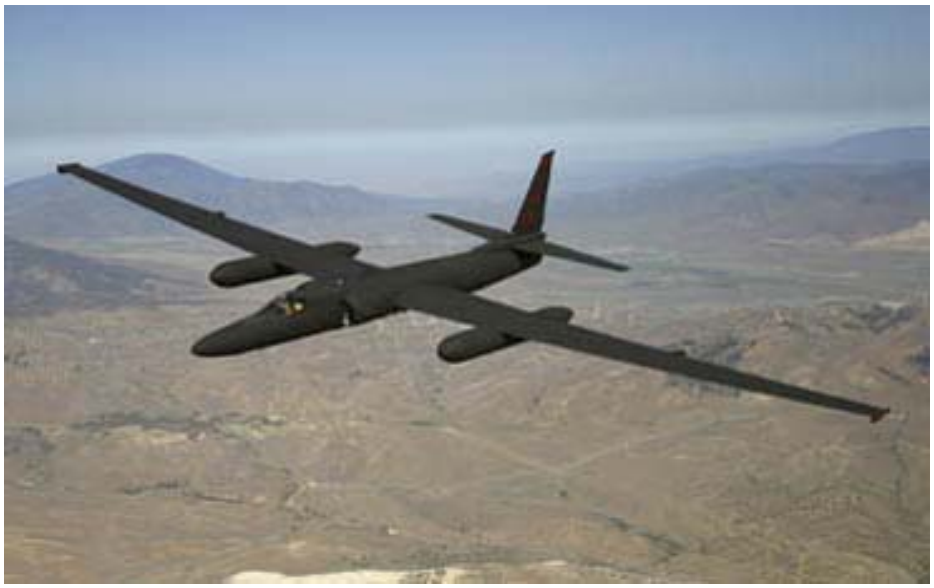


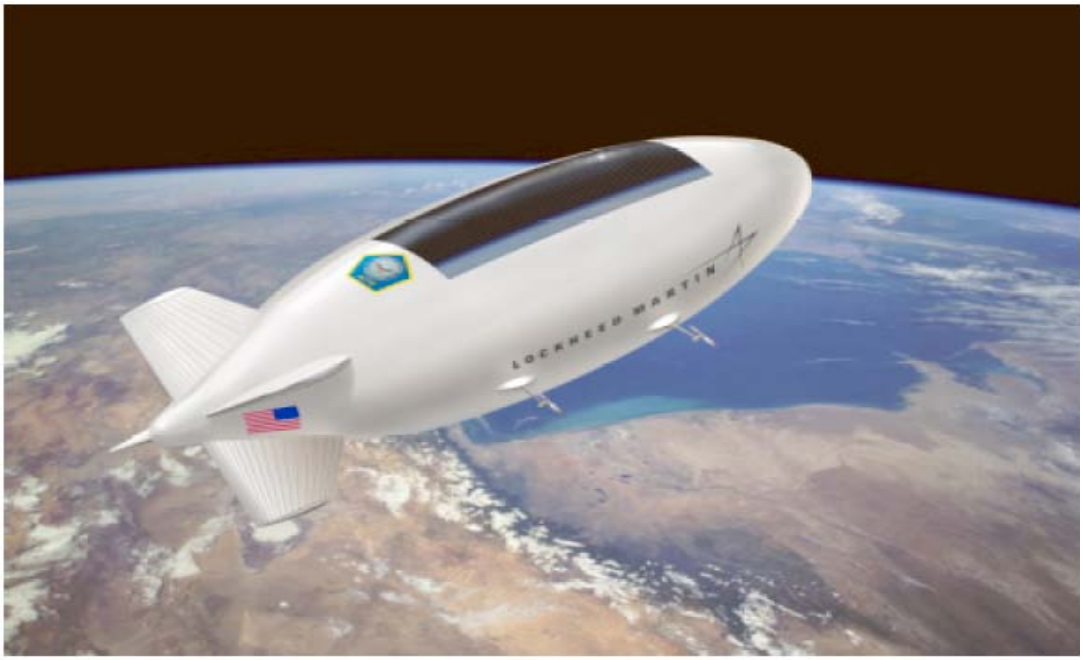
Figure 3. United States Air Force U-2, Dragon Lady
Source: United States Air Force, Fact Sheet, U-2 Dragon Lady; available from http://www.air-attack.com/page/55/U-2-Dragon-Lady.html; Internet; accessed on 25 May 2007.

The vehicles employed in this environment could travel to near space rapidly and inexpensively to provide many of the capabilities that troops and Soldiers currently demand (United States Air Force 2000c). More importantly, this near-space collection capability represents the most promising collection development for achieving persistent ISR. Two experimental concepts represent the DoD's potential for near-space operations: high-altitude-airship, and the near-space balloon.

High Altitude Airships

One promising LTA asset planned to operate in near-space is the High Altitude Airship (see figure 4). Airships are typically manned and utilize engines for propulsion. They have potential to be utilized for long-range aerial-surveillance, missile defense, weather observation, and aerial communication relay. The airship could power itself to

maintain time on station for months and the surveillance suite would extent coverage over the horizon to monitor a great surface area. An airship of this capability could be deployed to overlap coverage and extend surveillance over large surface areas like the US border (GlobalSecurity.org 2007).



SOURCE: U.S. Missile Defense Agency. Image courtesy Lockheed Martin Maritime Systems & Sensors.

Figure 4. High Altitude Airship
Source: Lockheedmartin.com. High Altitude Airship; available from http://www.lockheedmartin.com/wms/findPage.do?dsp=fec&ci=14477&rsbci=0&fti=0&ti=0&sc=400; Internet; accessed on 25 May 2007.

This capability could be likened to that of an inexpensive, geostationary satellite; the perfect asset for persistence. The main limiting factor is weight and the sensor payload it could carry (Bolkcom 2004, 5).

The Missile Defense Agency has funded an Advanced Concept Technological Demonstration to test the asset's ability to achieve objectives. The operational utility of the airship is less well understood than aerostats, so additional research is required to further refine the platforms potential contributions to the persistent network. The utility for homeland security is great. In addition, Lockheed Martin developed an unmanned airship that would operate above the jet stream and above weather to operate in a geostationary orbit at 70,000 feet. High Altitude balloons are currently closer to operational missions than the airship (Ison 2006, 28).

High Altitude Balloons

Balloons operating in near-space represent a very similar capability to the airship. Specially designed surveillance balloons could be floated up to near space in order to survey enemy territory in addition to executing other critical missions (see figure 5). The balloon represents a very low cost ISR and communication option which is currently undergoing testing for operational missions. The USAF Research Laboratory characterizes the potential of the high-altitude balloon as follows:

> High-altitude balloons and aerostats are low cost, non-polluting, vibration-free, and highly reliable platforms with quick response times, long duration flights, unlimited configurations, near unlimited launch sites, and fully recoverable payloads. Balloons can be used to simulate both low-earth orbit and geosynchronous satellites by taking advantage of repeatable stratospheric wind patterns. Space qualified hardware is not necessary. (United States Air Force 2007c)

The potential utility for executing persistent ISR missions in near-space onboard high-altitude balloons could be revolutionary in answering combatant commander's calls for persistence. Due to the platform's many advantages and low level of risk, the only true disadvantages will potentially be identified in operational testing.

Whichever of the two potential near-space capabilities is fielded first is not significant. The significance lies in the asset's capability to provide persistent target coverage. Both assets potentially have the capability of loitering over the target area for months at a time. And since the long-range optical equipment onboard is already proven from space, an even farther reaching atmosphere, the only seemingly outstanding barriers are in the funding, air vehicle construction and integration, and collection integration into the existing intelligence architecture.

Figure 5. Artist's Conception of the High-Altitude Airship High-Altitude Balloon
Source: United States Air Force, Fact Sheet, *Near Space Access Program*; available from http://www.vs.afrl.af.mil/FactSheets/near-space.html; Internet; assessed 5 February 2007.

The sum of these exciting and promising technologies will likely result in an incredibly robust collection capability no country has yet to experience. While the US has

arguably enjoyed an informational advantage over adversaries for decades, this current growth industry is attributed to a number of factors, but most importantly the US' most recent conflict; the GWOT. This war matches US informational superiority to a technologically savvy and illusive enemy: the global terrorist. Empowered by the Internet and an ability to melt into the population, the terrorist has exploited a weakness in US intelligence. Truly, uncovering terrorist activity is a difficult problem set; and American defense industry is targeting this problem set with new technologies ideally suited for the GWOT. Their utility, however, is not unilateral. Near-space technology could be applied to military problem sets and represent a significant stride towards employing persistence in any conflict.

However, the number of collection assets the US currently employs coupled with the potential of future developmental capabilities, could complicate the intelligence analyst's job beyond comprehension. The enterprise described is one potentially flooded with information but void of intelligence, and therefore knowledge. If not corrected, the US Intelligence Enterprise will only get more complicated to operate in and will likely be less effective in countering the global threat.

Better Methods of Passing Information

General Cartwright's first requirement in improving ISR called for more efficient ways to collect information. The general's second requirement to improve ISR was better ways to pass the information. While many technologies stand to greatly improve the collection capability of the US Intelligence Enterprise, the communication architecture and dissemination capabilities are also critical to the pursuit of persistent ISR. The core of this problem was previously identified by the *9/11 Commission Report*. Authors stated

that the information needed to link the 11 September plot together was in the hands of US analysts; it just was not in the hands of one analyst capable of piecing the puzzle together (National Commission on Terrorist Attacks 2004, 255). Since it was in the hands of many different analysts, it was divided information which never became intelligence. That is the focus required to address and correct this issue.

The issue goes beyond the need to just improve the passing of information. The issue is multifaceted and can be attributed to many of the historical constructs previously identified in this research. So how is it fixed? The answer is not simple. It will take an authoritative revolutionary change to fix an issue of this magnitude with so many different agencies and services having a stake in the outcome. To begin, the main problems prohibiting more robust sharing of information must be addressed.

Put One Agency in Charge

To begin with, there is no one element or agency in charge of US intelligence program acquisition and integration. The different services and agencies that regularly acquire intelligence collection assets have no incentive to ensure the integration of their respected intelligence acquisition programs. Each has a requirement to provide intelligence to their respected services and therefore purchase assets that enable that capability. And they need to do it at the lowest possible cost. There is no oversight agency with the authority to ensure their acquisition will contribute to the overarching US Intelligence Enterprise; to determine how its software will integrate with the "network;" and to determine if the acquisition is truly needed or if another enterprise asset could provide the same effect.

Director of National Intelligence

After 11 September occurred, the Congress and President Bush acted upon the recommendations of the 9/11 Commission and established the Director of National Intelligence (DNI) to act as the head of the National Intelligence Community. A position proposed as early as 1955, the DNI's authority was enacted through the *Intelligence Reform and Terrorism Prevention Act of 2004*. The DNI's responsibilities include: serving as the intelligence principal advisor to the President; serving as the head of the intelligence community; and directing the National Intelligence Program (US Congress, House 2004b, 7). Unfortunately, the DNI lacks the true authority that could provide oversight and integration required to link the community.

A cursory glance at the DNI's roles and responsibilities is misleading. While the DNI does control the National Intelligence Program (the National Intelligence Community's budget), he does not control the Military Intelligence Program (the budget authorizing military related intelligence activities; the Secretary of Defense controls the Military Intelligence Program. The DNI also lacks the authority to direct and control any element of the intelligence community except his own staff, and he has no authority to hire or fire anyone outside of his staff. While the position alludes to one of omniscient control of the intelligence community, this is not entirely accurate.

United States Strategic Command

Another player recently providing broad authority in the intelligence community is USSTRATCOM. The *UCP 2002*, and its Change 2, signed by President Bush in 2003; was one of the most significant alterations in how the DoD fights wars since the *Goldwater-Nichols Act of 1986*. One of those changes brought about was the assignment

of emerging mission areas to the functional combatant commands. The four emerging missions of global strike, information operations, missile defense and global C4ISR were assigned to USSTRATCOM responsibility (Garamone 2005).

UCP 2002 tasked USSTRATCOM to plan, integrate, and coordinate DoD ISR in support of strategic and regional operations (US Congress, House 2004a, 1). The command has faced this new tasking by integrating operations and intelligence into a single ISR division to increase synergy between those who determine collection requirements, those who collect, and the end users. Another monumental move was USSTRATCOM's creation of a Joint Functional Component Command for C4ISR led by the DIA and currently located in Washington, DC. This new focus represents USSTRATCOM's aim to develop a mission-centric process concentrating on global collection requirements, adjudicate regional combatant commanders, and national priorities, and seek better utilization of limited global ISR assets (Department of Defense 2004, 3). Therefore, the *UCP 2002* tasked USSTRATCOM to plan, integrate, and coordinate the intelligence effort on behalf of the DoD. However, the command has no approval authority on intelligence related plans and acquisitions the individual services make. This is a critical fault.

United States Joint Forces Command

The United States Joint Forces Command (USJFCOM), was also assigned a greater role in developing joint force ISR for the DoD. The staff at JFCOM summed it up appropriately:

> Taking guidance from the Unified Command Plan, the Defense Department's priorities, combatant commander requests, and operational lessons learned, JFCOM is working to "optimize joint intelligence"--allowing us to bridge the

> national to tactical gap. Specifically, the J2 is JFCOM's lead for Joint Operational Intelligence Transformation (JOLT); intelligence, surveillance, and reconnaissance (ISR); and battle damage and effects assessment (BDA/EA). Joint Forces Command works joint intelligence within four engines of transformation (joint concept development and experimentation; joint training and education; joint integration and interoperability; and as the global joint force provider) to support transformation and to deliver "born joint" products to the warfighter. (Wagner and Perkins 2004)

The DOD Strategic Planning Guidance 2006-2011 also directed JFCOM to provide a "strategy and roadmap to optimize joint operational intelligence." JFCOM also plans to transform operational-level intelligence and "ensure JFCOM efforts are in harmony with the Intelligence Community and are fully integrated and consistent with the overall transformation of DOD" (Wagner and Perkins 2004). Therefore, JFCOM is working intelligence transformation and joint integration. But what authority does a combatant commander, specifically JFCOM/CC, have over the services? None; therefore, this represents another example of a stake holder with little power in the overall DoD intelligence hierarchy.

As previously stated, the DoD has placed USSTRATCOM in charge of "synchronizing" and USJFCOM in charge of "optimizing" Joint intelligence operations across the department. Outside the realm of the DoD, the Director of National Intelligence is the appointed leader of the intelligence community. However, is anyone truly in charge? Is there one agency with the power to lead and integrate the entire US intelligence effort? There is currently no one agency or service, or national director, with enough power to significantly impact the required changes needed to achieve a persistent capability. There are simply too many players with their hands in the pie. One agency must have overarching authority to lead and integrate the complete intelligence effort; especially if the community aims to achieve persistence.

When there is decentralized execution with no centralized authority, it is difficult to achieve a common goal. Unfortunately, the multitude of agencies and services will fail to work together to maximize unity of effort if no one organization forces their hand. This is due to a myriad of reasons but the Intelligence Community as a whole will never achieve its true capability (persistent ISR) working disjointedly. An example is the US Army's recent purchase of the Warrior UAV.

In August of 2005, the US Army awarded General Atomics a $1 billion contract to provide 132 Extended Range Multi-Purpose Warrior UAVs to be operational by 2009 (International On-line Defense Magazine 2005). The move represents an US Army purchase of 132 UAVs that are nearly identical to the capabilities provided by the Predator UAV the USAF employs. When the US Army Comanche helicopter program was cancelled, the service had a significant amount of money in its coffers to spend. At about the same time, there was a call from the OIF and Operation Enduring Freedom theater for increased UAV support. This occurred at a time when USAF Predator UAVs were still coming onto the operational battlespace because they were such a new asset in the inventory. The USAF was fielding the assets as soon as they took delivery. It was a case of Soldiers on the field knowing how great a capability was so everyone wanted it, and rightly so. However, the Air Force could only field the assets on hand they had received from the manufacturer. So the US Army utilized this "requirement" for additional UAV capability and funded a practically identical capability to one employed by another service.

There are a few issues here. The first one is duplication of effort and waste; especially during a period when "joint warfighting" is adamantly touted as the way US

forces wage warfare. The second one is trust. If the services cannot trust one another to the point of spending $1 billion to provide a self-serving capability, the DoD lacks true jointness. The third and most significant in the effort to achieve a persistent ISR capability is that of integration. Adding an additional collection asset and its associated processing and dissemination nodes further complicates the integration solution needed to achieve persistence. This is because there is no one agency responsible for ensuring the Warrior UAV's collection is tied into overarching collection architecture. Will the intelligence community have access to the Warrior's collection? Where will the information be available to the joint user? The absence of an agency with the bureaucratic oversight and required power to effect decisions across intelligence organizations enables the duplication of effort and true waste that would infuriate the majority of taxpayers.

Title 10

A significant barrier to intelligence fusion unfortunately has to do with Title 10 authorities. Title 10 of the US Code outlines the role and authorities of the US armed forces. It provides the legal basis for the roles, missions, and organization of each of the services as well as the DoD (United Stated Code Title 10 1996). Title 10 basically tasks the armed services to organize, train, and equip their respected forces. The critical task amongst these three for obtaining a persistent ISR capability is equipping the force. Equipping means to provide a capability and providing a capability brings funding into the equation. Unfortunately, funding is a key barrier to achieving persistence.

When a service funds a collection capability, that capability will answer a critical requirement of that respected service. The critical requirement will be in direct alignment with that service's assigned roles and missions and will not necessarily be produced for

joint warfare. In other words, a service is not likely to spend the required dollars to ensure their new capability can be utilized by the other armed services. Linking their new capability into the joint services' communication and dissemination architecture can add significant amounts of funding to the bottom line. In addition, there is usually no agreed upon command and control architecture standard amongst the armed services.

While new service acquisitions must now navigate the Joint Capabilities Integration Development System ((JCIDS), the current joint requirements and procurement system) process for joint vetting, the process has the potential to act in the interest of the services and not be joint in nature. But more importantly, the manner in which Title 10 funding is designed limits the power of USSTRATCOM and JFCOM in integrating the intelligence community. The two organizations responsible for "synchronizing" and "optimizing" intelligence have little say in how the services spend their money under Title 10 authorities. While USSTRATCOM defines the missions and states the requirements for accomplishing those missions, it has no true authority over how the services spend their money. One USSTRATCOM action officer lamented that:

> We do have a small stick in the requirements process itself. As written requirements go thru the coordination process, if STRATCOM non-concurs on a requirements document, it stops until the Command's concerns are addressed--that is part of the JCIDS process. I can make recommendations in Integrated Priority Lists but I can't tell the Services how to spend their money. (Martin 2007)

Therefore, the two organizations tasked with improving intelligence collection for DoD have little impact in the assets and programs the services implement in relation to intelligence.

Whether or not USSTRATCOM agreed with the US Army's decision to purchase the Warrior UAV is irrelevant to this argument. The point of concern is what they

thought about the Army's decision based on how the new multimillion dollar asset was going to serve the JFC. Other points of concern were likely how the system's collected battlefield information will fit into existing dissemination architectures to ensure the information is not stove piped. A program of the Warrior's magnitude has the potential to greatly increase battlefield collection capability and a failure to plan and ensure its proper integration is a step in the wrong direction. As previously mentioned, although USSTRATCOM was recently charged with integrating US intelligence collection, they had no authority in how the Army spent the money left over from the cancelled Comanche program. This lack of authority represents the crux of the issue.

This example was not intended to unilaterally point blame at one service for purchasing ISR assets to support their operations; examples can be cited from every service. The intent was to highlight a larger problem in need of attention. Chapter 5 will further discuss the issue of authority and make recommendations on improving upon the changes implemented in 2002's UCP.

Findings

Chapter four outlined numerous issues that exist within the US intelligence community and stand as a barrier to achieving persistent ISR. These issues were identified by *The 9/11 Commission Report* and after combat operations in OIF I. In large part, the community suffers from a Cold War era designed architecture centered on dissecting the threat of the mighty Soviet Union. Today's threat based environment poses significantly different challenges demanding a persistent ISR capability. While the US currently fields a robust and capable intelligence collection capability, additional and more capable assets are required to obtain persistence. Exploiting the possibilities of

collection from near space and funding new technologies like airships and balloons can significantly enhance the collection capabilities of the community in its effort to obtain persistence. In addition, the community must find new methods for sharing and passing the enormous amounts of collection information to enable collaboration and perfect knowledge. Any semblance of the required institutions to ensure the intelligence community attempted to integrate efforts were absent until recently. Recent changes to the roles and responsibilities of USSTRATCOM and JFCOM, in addition to the appointment of the DNI, are a step in the right direction. However, more restructuring is required before the needed authorities are in place that will enable the integration needed for a persistence ISR capability.

The thesis' research question focused on whether or not the DoD can achieve a persistent ISR capability in the near term. Based on the research conducted in this chapter, the DoD cannot achieve a persistent ISR capability in the near future due to the lack of sufficient intelligence collection platforms and the disjointed nature of the intelligence community's command and control infrastructure as a whole. The next chapter will outline the conclusions and recommendations for obtaining a persistent ISR capability.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> The need for persistence from the ISR Enterprise is not new. However, numerous studies, experiments, and exercises over the years have failed to adequately determine the true nature of the problem of persistence and have consequently provided few answers or recommendations for solutions beyond simply increasing collection capability. (2006a, 14)
>
> Department of Defense
> Joint Staff Persistent ISR Joint Integrating Concept Paper

Conclusions

The above quote accurately summarizes the general perception of the persistent ISR dilemma. A topic search will reveal many calls for persistent ISR along with references on how certain assets will help obtain a future capability but there is an alarming void of material on actually achieving it. This can likely be attributed to the inability of the current command and control intelligence force structure to actually accomplish it. The time is long overdue for the community to look at the issue from a broader perspective.

Therefore, this thesis concludes that the DoD cannot achieve a persistent ISR capability in the near future due to the current lack of required collection capabilities and the inability of its intelligence community to integrate their efforts. The current lack of sufficient collection resources and the fragmentation existing in the intelligence community removes any hope of achieving a capability due to the requirement of a highly concerted command and control effort. This is where the solution resides. More

collection capabilities will be acquired. Future attention must be levied on the command and control of DoD intelligence as a whole.

Chapter 4 described the barriers hampering the achievement of a DoD persistent ISR capability. The chapter also outlined future collection technologies with the promise of enabling the achievement of the capability. General Cartwright's summary of the problems facing the intelligence community accurately and succinctly summarized the persistent ISR issue. In formulating his two main points on improving intelligence, he called for improving the way in which information is collected and the ways information is passed. While a simplified summary, the two points are a direct synopsis of the challenges facing the community if it desires relevance in future combat operations.

Improvements to the way information is collected are primed to be fielded in the near future. Stated another way, the DoD will continue to research, develop, and field new and highly improved intelligence collection capabilities. Indeed, as long as the required funding remains available, many new technologies stand to vastly advance the manner and volume in which information is collected and processed. The immediate problem lies in how these new technologies are acquired and structured into the force. To realize their true potential and gain momentum towards a persistent ISR capability, these new capabilities must be smartly acquired, integrated, and controlled by the intelligence community. This requires a centralized authority empowered to conduct all the above stated duties.

Recommendations

With the services retaining responsibility for their inherent ISR capabilities, each service will continue to acquire individual ISR platforms. This results in the status quo.

The research revealed that numerous problems exist in the Intelligence Enterprise that inhibit a persistent ISR capability. The problems specific to DoD include a high degree of competition between the services for ISR missions; the fielding of numerous platforms with the same capability resulting in lost efficiency; high cost resulting in the lost opportunity of acquiring a greater capability benefiting the entire Joint Force; and confusion over which service is responsible for what mission.

These discrepancies are a waste to the American taxpayer and reveal an organization weeping for restructuring, reorganization, and new leadership. Recent discoveries and current operations highlight the importance intelligence plays in the successful defense of this country. Indeed, the GWOT will be won only with the successful use of America's vast intelligence assets. Intelligence operations are too complex and require such significant planning and oversight that the current dismembered organization must be restructured. In addition, for the community to realize its full potential and support the country with a persistent ISR capability, it must be unified.

In an effort to unify the numerous and diverse intelligence efforts in DoD, the *UCP 2002* directed USSTRATCOM to lead the intelligence effort for the entire Joint Force. While a valiant attempt to correct current faults, it is not enough. USSTRATCOM currently lacks sufficient power and funding oversight to truly bring about significant change. As previously stated, USSTRATCOM can provide direction and guidance but they are absent the required power to direct the DoD's collective funding for intelligence collection platforms. This results in the services funding their individual intelligence related programs to benefit their unique collection requirements.

With no true centralized authority obtaining the power to control the vision and the funding of intelligence acquisitions, the ISR Enterprise will never be capable of achieving the synchronization required to realize persistence. If DoD's leaders truly desire this capability, and one supposes they do given the amount of outcry and combatant commander's stated requirements, significant change is required.

The significant change required to realize a persistent ISR capability is for the DoD to centralize the command and control of Defense Intelligence; specifically acquisition and integration efforts of the entire Department. The DoD already has multiple agencies in the intelligence business and each one of the services also has an intelligence arm. This represents incredible duplication of effort and a waste of resources. In addition, as these agencies and the Services compete for limited funding with overlapping missions and assets capable of completing the same missions, ensuring the synchronization of different missions and capabilities could reap numerous benefits.

One recommendation is to designate a DoD component as its Executive Agent for Intelligence Acquisition to oversee all acquisition and integration of Joint Intelligence capabilities. This agent must have the authority to approve and disapprove service intelligence acquisition programs. The Secretary of Defense or Deputy Secretary of Defense maintains the authority to designate a DoD component as DoD's Executive Agent for a "specific responsibility, function, and authority to provide defined levels of support for operational missions, or administrative or other designated activities that involve two or more of the DoD components" (Department of Defense 2002, 2). The designated authority would yield significant power in the Department and over the Services while ensuring a joint approach to the fielding of the appropriate mix of

intelligence assets to answer the JFC's intelligence requirements. While a specific service could act as the Executive Agent, an appropriate choice for this position would be the Undersecretary of Defense for Intelligence (USDI) or the Director, DIA.

A relatively new position in the DoD, the position of USDI was created in 2003 "in order to have a single office overseeing the organization, planning and execution of military intelligence missions" (SourceWatch.org 2007). If specifically directed and empowered, the USDI could direct all service acquisitions and integration to meet these objectives and ensure joint coordination amongst the individual services. This appointment would centralize the decision making process and place one individual in charge of ensuring the four services work together to accomplish the joint vision of acquiring a persistent ISR capability. Without this centralized authority, achieving the capability is unattainable. With centralized acquisition authority for intelligence collection platforms, the USDI can ensure acquisitions fit into an approved and synchronized persistent ISR structure and architecture. Reducing duplication of effort is a goal the department can not afford to ignore.

The DIA is a combat support agency directly tied to support of military intelligence operations. Its mission has traditionally revolved around providing intelligence support to the military; however, its strong capability and background represent an agency ideally suited to assume a greater role of leadership in the DoD. The Director of DIA is a three-star military officer who serves as principal adviser to the Secretary of Defense and Chairman of the Joint Chiefs of Staff on matters of military intelligence, therefore, the Director is already serving in an advisory role to the SECDEF and has assumed limited leadership over the Service's Intelligence operations (Defense

Intelligence Agency 2007). Either option would benefit the community as a whole, however, the resounding point is there must be centralized control over intelligence acquisition to enable the enterprise to obtain a greater capability.

Chapter 4 outlined an effort by the Joint Staff to integrate collection management processes across the services. This effort is referred to as the Persistent ISR Joint Integrating Concept. In summarizing the risks of not incorporating the changes recommended in the Joint Integrating Concept, the author provided a striking summary that can also be applied to the proposed centralization of DoD's acquisition authority.

> Overall, the risk of not integrating collection management strategies for the ISR Enterprise will at the very least do nothing more than compound existing problems. For example, we continue to field more and more collection capabilities with little regard for how they "plug-in" to the ISR Enterprise as a whole. This activity will continue to overwhelm an already undermanned intelligence force with a deluge of information that is at best duplicative and/or unnecessary. (Department of Defense 2006b, 14)

The effort to obtain a persistent ISR capability has reached a similar point. To continue on the same path will just compound the existing problems of the enterprise. That issue is what drove the Joint Staff to single out and tackle only the collection management portion of the intelligence cycle with the Joint Integrating Concept.

This method of approach only addresses the intelligence organizations in the DoD; specifically the intelligence arms of the armed services. The creation of the Director of National Intelligence post is the first attempt at the national level to integrate the intelligence organizations of the country. While somewhat restricted by the political nature of the decision, this post has the potential to alter the manner in which the varied organizations work together. However, it is quite interesting that it took the President of the US to alter the organizational structure required to make these organizations work

together. The same type of revolutionary change is required for the DoD and the decision must come from the highest echelons of government.

The first step is the realization that a true persistent ISR capability is impossible under the current command and control structure. Among business and military type organizations, the intelligence business and culture is one not conducive to numerous organizations conducting various missions that often overlap. A more centralized approach is required to guarantee fusion, coordination, and information sharing among US intelligence capabilities. This approach, if grasped, would truly saddle the vast and capable intelligence collection capability of the world's most formidable superpower. It would also ensure the proper creation, acquisition, and integration of promising future collection technologies. This path will soon enable a persistent ISR capability that would allow an all-seeing eye over modern day adversaries and ensure victory in the battle space of tomorrow.

REFERENCE LIST

Abatti, James M. 2005. Small power: The role of micro and small UAVs in the future. Research Report, Air Command and Staff College, Maxwell AFB, AL.

Bolkcom, Christopher. 2004. CRS Report for Congress RS21886, Potential Military Use of Airships and Aerostats. Washington, DC: Government Printing Office. 2004.

Boyne, Walter J. 2003. *Operation Iraqi Freedom: What went right, what went wrong, and why*. New York, NY: Forge.

Bradley, Carl M. 2004. ISR in support of operation Iraqi freedom: Challenges for rapid maneuvers and joint C4ISR integration and interoperability. Research Project, Naval War College, Newport, RI.

Brinton, John H., Major and Surgeon U.S.V. 1914. *Personal memoirs of John H. Brinton*. Neale Publishing Company. Available from http://books.google.com/books?id=jy4JAAAAIAAJ&pg=PA5&dq=Memoirs+of+John+H.+Brinton+&psp=1#PPA17,M1. Internet. Accessed 25 May 2007.

Chizek, Judy G., Jennifer Elsea, Richard A. Best, Jr. and Christopher Bolkcom. 2003. *Military transformation: Current issues in intelligence, surveillance, and reconnaissance*. Hauppauge, NY: Novinka Books.

Cornell Law School. *United States Code* Title 50, Chapter 15, Subchapter 1, National security council. Available from http://www.law.cornell.edu/uscode/search/display.html?terms=transnational%20threat&url=/uscode/html/uscode50/usc_sec_50_00000402----000-.html. Internet. Accessed 22 December 2006.

Cunningham, Kevin R. 2001. The changing relationship between intelligence and strategy: Paradoxes and possibilities. Research Project, US Army War College, Carlisle Barracks, PA.

Defense Industry Daily. 2007. Warrior ERMP: An enhanced predator for the army. Available from http://www.defenseindustrydaily.com/2007/02/warrior-ermp-an-enhanced-predator-for-the-army/index.php. Internet. Accessed 3 February 2007.

Defense Intelligence Agency. 2007. *Introduction to DIA*. Available from http://www.dia.mil/thisisdia/intro/index.htm. Internet. Accessed 25 May 2007.

Department of Defense. 2001. News transcript: DoD news briefing-General Richard B. Myers, Joint Chiefs of Staff. Available from http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=2632. Internet. Accessed 25 May 2007.

_____. 2002. Department of Defense Directive 5101.1, *DoD executive agent.* Washington, DC: Government Printing Office.

_____. 2004. *Defense science board task force report on enabling joint force capabilities-Phase II.* Washington, DC: Government Printing Office.

_____. 2006a, *Persistent intelligence, surveillance, and reconnaissance: planning and direction, joint integrating concept* Version 0.7. Washington, DC: Government Printing Office.

_____. 2006b. *Persistent intelligence, surveillance, and reconnaissance: planning and direction, joint staff joint integrating concept* Version 0.9. Washington, DC: Government Printing Office.

Dorr, Robert F. 2006. "No plane is ready to fill U-2's hangar quite yet." *Air Force Times*. Available from http://www.airforcetimes.com/legacy/new/0-AIRPAPER-2163292.php. Internet. Accessed 3 February 2007.

Garamone, Jim. 2005. "U.S. Strategic Command Transforming, decentralizing." *Armed Forces Press Service.* Available from http://www.af.mil/news/story.asp?storyID=123010426. Internet. Accessed 22 May 2007.

GlobalSecurity.org. Intellegence, high altitude airship. http://www.globalsecurity.org/intell/systems/haa.htm. Internet. Assessed 4 February 2007.

Harshberger, Edward R., Director of the Strategic and Doctrine Program of Project Air Force at RAND. 2002. *Global implications for the U.S. Air Force*. Available from http://www.rand.org/publications/randreview/issues/rr.08.02/global.html. Internet. Accessed on 25 May 2007.

Hermann, Robert, and General Larry D. Welch, USAF (Ret.). 1997. *Report of the defense science board 1996 task force on C4ISR integration*. Washington, DC: Defense Science Board.

International On-line Defense Magazine. 2005. "EMRP: extended range multi-purpose UAV." *Defense Magazine*, no. 2. Available from http://defense-update.com/products/e/ermpUAV.htm. Internet. Assessed 11 March 2007.

Ison, David. 2006. "Persistent coverage." *C4ISR Magazine*, 5, no. 9: 28.

Joint Chiefs of Staff. 2001. Joint Publication 1-02, *Department of defense dictionary of military and associated terms*. Washington, DC: Government Printing Office (as amended through 22 March 2007).

_____. 2004. Joint Publication 2-01, *Joint and national intelligence support to military operations*. Washington, DC: Government Printing Office.

Kirtland Air Force Base. Fact Sheet. *Near space access program, high-altitude balloons and tethered aerostats*, http://www.kirtland.af.mil/library/factsheets/factsheet.asp?id=7890. Internet. Accessed 23 May 2007.

Kissinger, Henry A. 2001. *Does america need a foreign policy?* (New York, NY: Simon and Schuster.

Larson, Eric, Derek Eaton, Paul Elrick, Theodore Karasik, Robert Klein, Sherrill Lilngel, Biran Nichiporuk, Robert Uy, and John Zavadil. 2004. *Toward a long-term strategy for assuring access in key strategic regions*. Santa Monica, CA: RAND Corporation.

Martin, Stuart, USSTRATCOM J841. 2007. Telephone interview by author, 16 February, Leavenworth, KS.

Moseley, Michael T., Lieutenant General, USCENTAF, Assessment and Analysis Division. 2003. Operation Iraqi freedom: By the numbers. Available from http://www.globalsecurity.org/military/library/report/2003/uscentaf_oif_report_30 apr2003.pdf. Internet. Accessed on 25 May 2007.

Myers, Richard B., General. 2004. "A word from the chairman, shift to a global perspective." *Air and Space Power Journal* 17, no. 3 (September): 5-10.

National Commission on Terrorist Attacks. 2004. Final report of the national commission on terrorist attacks upon the United States: *The 9/11 commission report*. Washington, DC: Government Printing Office.

Committee on C4ISR for Future Naval Strike Groups, National Research Council. 2006. *C4ISR for future strike groups*. Washington, DC: National Academy Press.

Pendall, David W., Major, U.S. Army. 2005a. "Persistent surveillance and its implications for the common operating picture." *Military Review*, 85, no. 6 (November-December): 41-51.

_____. 2005b. The promise of persistent surveillance: what are the implications for the common operating picture. Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Posen, Barry R. 2001/2002. "The Struggle against Terrorism: Grand Strategy, Strategy, and Tactics." *International Security* 26, no. 3: 39-55.

Rockwell, David L., Teal Group. "US airborne ISR market." *The Journal of Electronic Defense* 28, no 10 (October 2005): 46-49.

Rowe, Bruce. 2006. "The big picture: Airship gives Marines a view of the urban battlefield." *C4ISR Magazine* 5, no. 4 (May): 32-33.

Sloan, Elinor C. 2005. *Security and defense in the terrorist era (foreign policy, security, and strategic studies)*. Canada: McGill-Queen's University Press.

Source Watch. 2003. Undersecretary of defense for intelligence. Available from http://www.sourcewatch.org/index.php?title=Undersecretary_of_Defense_for_Intelligence. Internet. Assessed 17 May 2007.

Stephens, Hampton. 2005. "Near space." *Air Force Magazine* 88, no. 7. Available from http://www.afa.org/magazine/July2005/0705near.asp. Internet. Accessed 23 May 2007.

Sun Tzu. *The art of war*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971.

Tirpak, John A. 2006. "Eyes of the fighter." *Air Force Magazine*, 89, no. 1. Available from http://www.afa.org/magazine/jan2006/0106fighters.asp. Internet. Accessed 3 February 2007.

Tomes, Robert R. 2003. "Informing US national security transformation discussions:an argument for balanced intelligence, surveillance and reconnaissance." *Defence Studies*, 3, no.2: 21.

TopIVision.com. Images. Available from http://www.topivision.com/Images/Aerostat/2.jpg. Internet. Accessed 25 May 2007.

Touchstone Pictures. 1998. "Enemy of the state." Available from http://www.movieweb.com/movies/film/35/1935/summary.php. Internet. Accessed 3 March 2007.

United States Air Force. 2007a. Fact sheet: Global hawk, http://www.af.mil/factsheets/factsheet.asp?fsID=175. Internet. Accessed 3 February 2007.

_____. 2007b. Fact sheet: MQ-9 reaper unmanned aerial vehicle. Available from http://www.af.mil/factsheets/factsheet.asp?id=6405. Internet. Accessed 3 February 2007.

_____. 2007c. Fact sheet: Near space access program. Available from http://www.vs.afrl.af.mil/FactSheets/near-space.html. Internet. Assessed 5 February 2007.

_____. 2007d. Fact sheet: Tethered aerostat radar system. Available from http://www.af.mil/factsheets/factsheet.asp?id=3507. Internet. Assessed 4 March 2007.

_____. 2007e. Fact sheet, U-2 dragon lady. Available from http://www.air-attack.com/page/55/U-2-Dragon-Lady.html. Internet. Accessed on 25 May 2007.

_____. 2007f. Photo by Chad Bellay. Available from http://www.af.mil/photos/index.asp?galleryID=47&page=1. Internet. Accessed 25 May 2007.

United States. 1996. *Title 10, United States Code: Armed Forces*. Washington: DC: Government Printing Office.

US Congress. House. Committee on Intelligence Technical and Tactical Subcommittee on Intelligence, Surveillance, and Reconnaissance. 2004a. Statement of Lieutenant General Thomas B. Goslin, USAF, Deputy Commander of United States Strategic Command. *Hearings before the House Permanent Select Committee on Intelligence Technical and Tactical Subcommittee on Intelligence, Surveillance, and Reconnaissance,* 108th Cong., 1st sess.

_____. House. 2004b. *Intelligence reform and rerrorism prevention act of 2004*. 108th Cong., 2nd sess., Report 108-796.

US Congress. Senate. Armed Services Committee. 2003. Summary of Lessons Learned. *Prepared Testimony by SECDEF Donald H. Rumsfeld and General Tommy R. Franks to Senate, Armed Services Committee*.

_____. Senate. Armed Services Committee. 2004. *Defense intelligence reorganization: hearings before the senate armed services committee,* 108th Cong., 2nd sess.

Wagner, Robert, Lieutenant General, and Colonel Stephen P. Perkins. 2004. "Joint Intelligence Transformation--Bridging the Gap." *Military Intelligence* 3, no.3 (July-September): 6-10. Available from http://www.fas.org/irp/agency/army/mipb/ 2004_03.pdf. Internet. Accessed 13 March 2007.

Welch, Larry D., General USAF (ret.), and Dr. Robert Hermann. 2004. *Defense science board task force report on enabling joint force capabilities: Phase II*. Washington, DC: Defense Science Board.

Welch, Paul A. Major, USAF. 2005. Global ISR: A process-oriented approach to achieving decision superiority. Research Program, Air Command and Staff College Maxwell AFB, AL.

Wikipedia, the Free Encyclopedia. 2007a. Non-state actor. Available from http://en.wikipedia.org/w/index.php?title=Non-state_actor&oldid=131774597. Internet. Accessed 21 May 2007.

_____. 2007b. State actor. Available from http://en.wikipedia.org//index.php?title=State_actor&oldid=104687397. Internet. Accessed 21 May 2007.

_____. 2007c. Unmanned aerial vehicle. http://en.wikipedia.org/w/index.php?title=Unmanned_aerial_vehicle&oldid=112143771. Internet. Accessed 3 March 2007.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Dr Jack D. Kem
DJMO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

Mr Russell H. Thaden
DJMO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

Lt Col Stephen E. Ramer
Air Force Element
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 15 June 2007

2. Thesis Author: Major Todd C. Hogan

3. Thesis Title: The Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority?

4. Thesis Committee Members: _____

Signatures: _____

_____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).